Establishing trust through provably fair bets backed by an open-sourced, verifiable smart contract in the Ethereum Blockchain.

Federick Joe P. Fajardo, eric@arpa.ph, November 2020

ABSTRACT

Trust is an essential part of every transaction whether it is interpersonal or computational. The trust involved in interpersonal relationships allows social associations and quality interactions between people. The same principle enables computer networks to have a symbiotic connection. There are two major factors or components that inherently build trust: fairness and equal opportunity. The goal of this paper is to formulate a method of establishing these factors in computer networks to elevate the trust between human actors and blockchain networks. Utilizing the classic game of Dice, which is widely played in physical and online casinos, the author of this paper aims to create a proof-of-concept that will serve as a reliable working model for a decentralized application on the Ethereum network.

INTRODUCTION

Personal relationships require trust to remain functional. As we design technologically advanced and more complex computer systems, this fundamental aspect of human relationship will need to be integrated to encourage public consumption and ensure the network's reliability.

In 1962, Edward Thorp expressed the casinos' consistent advantage in the game of BlackJack in his book entitled *Beat the Dealer* where he also mentioned strategies to increase the player's likelihood of winning. Similar to Blackjack, most gambling games have a working model that prevents the house from losing money against gamblers.

To combat this lack of equality, this paper will talk about the game of Dice, which is a common casino game that depends heavily on chance. It typically has little to no house advantage although this may differ depending on its construction and/or execution (Webb, 2002). The next sections of this paper aim to discuss how blockchain technology can address this fallibility, promote fair play, and even be the better medium for these games.

ESTABLISHING TRUST

The most common misconception about the blockchain network is that it is a 'trustless technology' because it eliminates the need for a third party to oversee transactions (De Filippi et al., 2020). Given this presumption and the anonymity feature in the network, malicious actors are motivated to develop fraudulent cryptocurrency assets and projects to deceive consumers. Although known companies try to counter this with transparency, the notion of a trustless system still leads the majority to avoid the said technology.

De Filippi et al. (2020) continue to argue that the network does not remove the impression of trust, but instead increases it by aggregating the confidence of consumers through its governance structure, which equally distributes power among all actors. This prohibits a single actor, with personal interests and objectives, to influence transactions and outcomes. Thus, to establish trust in online gambling games, a decentralized application that runs on the blockchain network may be utilized.

The Byzantine Generals' Problem

One example of an underlying problem of trust in distributed systems is the Byzantine Generals' Problem. This is a fundamental problem in distributed computing which focuses on the need of achieving reliability within multiple faulty processes (Lamport, 1983). These abstract problems can be summarized to the following needs:

- *Consensus:* Each general has to decide if they will attack or retreat, similar to a yes or no question. All generals must be in agreement with the final decision.
- *Finality:* That decision will then be executed by subordinates that fully trust the generals as the men perceive them to be loyal, authentic, correct and true.
- *Immutability:* Once the decision has been executed, no single component can alter the state of its execution.

In order to achieve victory, trust in the system must be existent. No traitor generals should be able to prevent the loyal generals from reaching a consensus. Similarly, messages that are relayed from one loyal general to another must be trustworthy and are not subjected to disruption. These relayed messages should have the essence of integrity and confidentiality working together.

Therefore, for trust to be established, the system and its actors must act in accordance with the principle of fairness and equality which is proven necessary in algorithmic decisions (Kasy & Abebe, 2020).

FAIRNESS AND EQUALITY

Much of the debate on the impact of algorithms is concerned with fairness, defined as the absence of discrimination for individuals with the same “merit" (Kasy & Abebe, 2020). Indeed, structures and distribution of power have the capacity to cause or reduce inequalities.

Given the structure of the game of Dice that greatly relies on statistical probability to arrive at a specific number, this reduces the risk of foul play as succeeding digits will be impossible to predict by players or even the host in physical casinos. Integrating the game of dice with a provably fair algorithm may allow the game to be fair and equal.

Provably fair algorithms are algorithms which can be examined and verified on the part of the service operator. These are often used by online casino operators and cryptocurrency gambling sites.

To achieve fairness, a method of verifying every transaction in the game will be published by the service operator including the generation and hashing of random numbers and the corresponding seed which will provide transparency. A third party provider called an *oracle* will be used for the Random Number Generations *(RNGs)*. When a game is played, the player will be setting their bets and the system will be using the algorithms to execute the bets and evaluate the results.

Anonymity is natively provided to everyone that plays the game. With this regard, there are no deposits or signups required compared to regular online and physical gambling operations. This promotes equal opportunity for everyone.

Furthermore, as the game will be on a decentralized application that runs on the blockchain network, no single person may be able to influence the application's structure or results without leaving a trace on the blockchain transaction ledger.

The Law of Large Numbers

The law of large numbers is important because it guarantees stable and long-term results for the averages of some random events. (Yao, K & Gao, J., 2016).

In probability theory, the law of large numbers states that the average of the results obtained from a large number of trials should be and will be close to the expected value as more trials are performed (Dekking, 2005).

Here, the random variable will be represented with *X* and the expected value with *E*.

$$X, E(X)$$

The *n* observations of our random variable *X* is the mean and will be represented as:

$$\overline{x}_n$$

Once observations have been gathered as portrayed by X_1+X_2+...+X_u, this will be divided by the total number of observations depicted by *n*. The answer to the equation would provide the value of the sample mean.

$$\overline{X}_n = \frac{x_1 + x_2 + \ldots + x_u}{n}$$

Based on this equation, the sample mean will reach the expected value of the random variable.

$$\overline{X}_n \to E(X)$$

Or the sample mean will reach the population mean for *n* approaching infinity.

$$\overline{X}_n \to u \text{ for } n \to \infty$$

On a classic game of Dice, a casino may lose money in a single roll. While the game parameters may eventually overcome any winning streaks by the player, the law only applies when a large number of observations is considered. (Wikipedia Contributors, 2020).

PROOF OF CONCEPT

We will be examining a decentralized application called Arpa Games as a proof of concept for this paper. This open source project was designed and forked based on the decentralized application Etheroll.

Etheroll is an Ethereum-based, dice gambling decentralized application built entirely on top of the Ethereum blockchain. Thus, it allows a certain level of transparency and accountability that traditional online casinos do not provide (Etheroll, 2017).

In order to examine and prove the probability of randomness of the games' outcome, we will be simulating the winning and losing scenario of the game on a roll under 51 which entails a 50/50 chance. Thus, in order for the player to win, the result must be equal to or less than 50.

We simulated bets by generating 188 random numbers from random.org. These random numbers were based from a fair, theoretical ninety four-sided dice that produces one of the numbers 2 to 95 for each roll.

https://www.random.org/integers/?num=188&min=2&max=95&col=1&base=10&format=plain&rnd=new

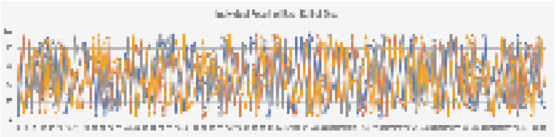
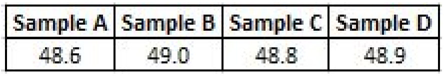


Figure (A). Shows the randomness of four (4) samples of 188 random rolls from numbers 2 to 95.

Here, the sample mean is represented by the below equation where the expected value is ± 48.5.

$$\overline{X}_n = \frac{2+3+\ldots+95}{94} = 48.5$$

Thus, the following results shows that based from the four (4) samples containing 752 rolls which is equivalent to 188 rolls for each sample, an expected value of ± 48.5 were achieved.



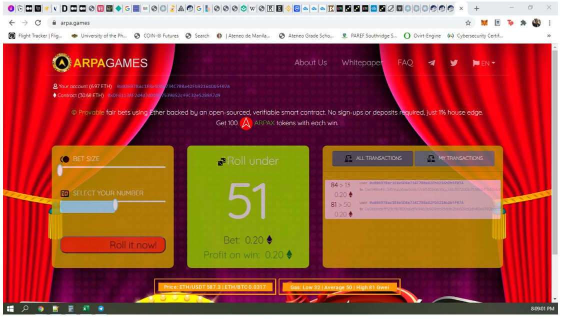
Sample A	Sample B	Sample C	Sample D
48.6	49.0	48.8	48.9

Figure (B). Shows that each result of the samples that were done were close to the expected value.

The Game Procedures

In order to play, the player must open the application https://arpa.games/ to launch the game. There will be three (3) parameters for the game to execute a bet.

- *Bet Size:* This is the size of the wager in Ether (ETH). Ether is the unit of cryptocurrency used in the Ethereum blockchain.
- *Roll Under:* If order to win, the player must roll the dice under this value.
- *Wallet Balance:* The wallet must have enough balance to make a bet and pay the Ethereum gas.



arpa.games

Your account (6.97 ETH) 0x08697Bac1E8e5D8e734C7BBa42Fb9216bDb5f07A
Contract (30.68 ETH) 0xDF6113AF2d4d3dD8987539852cf9C32e5289A7d9

© Provable fair bets using Ether backed by an open-sourced, verifiable smart contract. No sign-ups or deposits required, just 1% house edge.
Get 100 ARPAX tokens with each win.

BET SIZE
SELECT YOUR NUMBER

Roll under
51
Bet: 0.20
Profit on win: 0.20

84 > 13 0.20
81 > 50 0.20

Price: ETH/USDT 587.3 | ETH/BTC 0.0317
Gas: Low 32 | Average 50 | High 81 Gwei

Figure (C). Shows the user interface for the Arpa Games decentralized application.

Considering that there are enough funds in the cryptocurrency wallet, the player may initiate a bet by determining the bet size and the roll under.

The connected wallet will submit this to the blockchain network for processing and the transaction hash will remain to have a pending status. Once the transaction has been mined, it will be added to the block and the status will be marked as a success. The smart contract will take the bet and will request an encrypted random number from the oracle which is Provable.

In the blockchain space, an oracle is a party which provides data. Considering that blockchain is a separate network, external data is needed to be accessed such as price feed for financial applications and random number generation (RNGs) for gambling. However, relying on a newly trusted intermediary like an oracle would reduce the security and trust model of the blockchain application.

To make this work, the solution is to prove the authenticity of the data fetched from the data-source. This is accomplished by accompanying the returned data with a document called an authenticity proof which signifies the data integrity (Provable Documentation, 2015).

The code below shows the playerRollDice function:

```
function playerRollDice(uint rollUnder)
public payable gameIsActive
betIsValid(msg.value, rollUnder)
{

bytes32 provable_qryId =
provable_newRandomDSQuery(
QUERY_EXECUTION_DELAY,NUM_RANDOM_BYTES_REQUE
STED,GAS_FOR_PROVABLE_CALLBACK
);

queries[provable_qryId] = true;
playerBetId[provable_qryId] =
provable_qryId;
playerNumber[provable_qryId] = rollUnder;
playerBetValue[provable_qryId] = msg.value;
playerAddress[provable_qryId] = msg.sender;
playerProfit[provable_qryId] = ((((msg.value
* (100-(safeSub(rollUnder,1)))) /
(safeSub(rollUnder,1))+msg.value))*houseEdge
/houseEdgeDivisor)-msg.value;

maxPendingPayouts =
safeAdd(maxPendingPayouts,
playerProfit[provable_qryId]);

if(maxPendingPayouts >= contractBalance)
revert();
emit LogBet(playerBetId[provable_qryId],
playerAddress[provable_qryId],
safeAdd(playerBetValue[provable_qryId],
playerProfit[provable_qryId]),
playerProfit[provable_qryId],
playerBetValue[provable_qryId],
playerNumber[provable_qryId],
provable_qryId, BET_SENT_FOR_NUMBER);
}
```

Once the transaction has been mined, This will be returned to the user interface. The status will be marked with two question marks *"??"* which signifies that the random number from Provable is not yet known.

When Provable executes a call and sends the encrypted value, the smart contract finishes the game and returns the number. From there, it will be decided if it's a win or a loss.

If a bet is won, the house will not be taking the wager and the profit will be sent to the player's address together with the affiliate token. The affiliate token is a reward token that will be sent from the smart contract to the winning player's address. This is an ERC20 cryptocurrency asset which can be used for multiple purposes.

In a player winning scenario, the following computation will be as follows:

```
Roll under 50. Result = 47
BS = 0.20 / PW = 0.20 (THE PLAYER WIN)
BEFORE          AFTER
Player  01.01 + 0.19   = 01.20 ETH
House   36.68 - 0.21   = 36.47 ETH
Token   50000 - 100    = 49,900 ARPAX
```

In a house winning scenario, the following computation will be as follows:

```
Roll under 50. Result = 87
BS = 0.20 / PW = 0.20 (THE HOUSE WIN)
BEFORE          AFTER
Player   01.20 - 0.20  = 01.00 ETH
House    36.47 + 0.19  = 36.66 ETH
Tokenb   50000 - 0     = 50,000 ARPAX
```

CONCLUSION

Over the years, many physical establishments of business have transitioned completely or partially online especially during the COVID-19 pandemic. An example would be casinos currently having online websites/applications that offer the same games one would see in a physical house. As a significant amount of the public is now preferring online rather than face-to-face, it is indisputable that there is a need to create a sound business model to build trust between the system and consumers. This will also allow developers to maximize the benefits and minimize the downsides of the system.

In a September 2017 interview by Bloomberg with JPMorgan CEO Jamie Dimon, he argued that Bitcoin was a “fraud” and was worse than the Dutch tulip bulb market bubble of the 1600s (Jamie Dimon Slams Bitcoin as a ‘Fraud,’ 2017).

In January 2018, in an interview with FOX Business’s Maria Bartiromo, Dimon said that he regretted his previous comments about Bitcoin, and expressed his faith in blockchain technology (Martin, 2018).

In February 2019, JPMorgan made a surprising announcement that it has created a cryptocurrency called JPM Coin to facilitate instantaneous transfer of payments between their institutional accounts (J.P. Morgan Creates Digital Coin for Payments, 2020).

Considering that Bitcoin was the first actual use case of the blockchain network, this obvious move by large financial institutions such as JPMorgan signifies that they are able to see the value with this type of technology.

While there is always risk involved in every transaction, this growth opportunity can be an open invitation for other multinational industry players to see the advantages of such technology which can be applied as an improvement or solution to provide an improved trust model.

REFERENCES

Kasy, M., & Abebe, R. (2020). Fairness, Equality, and Power in Algorithmic Decision-Making. Retrieved November 14, 2020, from https://www.cs.cornell.edu/~red/fairness_equality_power.pdf.

Thorp E., Beat the Dealer: A Winning Strategy for the Game of Twenty-One, ISBN 0-394-70310-3.

De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. Technology in Society, 62, 101284. https://doi.org/10.1016/j.techsoc.2020.101284.

Lamport, L. (1983). The Weak Byzantine Generals Problem. Journal of the ACM, 30(3), 668–676. https://doi.org/10.1145/2402.322398.

Webb, D. (2002). Method and apparatus for playing a dice game. Retrieved November 16, 2020, from https://patents.google.com/patent/US6464225B1/en.

Miras, A. (2017). Etheroll whitepaper - whitepaper.io. WhitePaper.Io. https://whitepaper.io/document/472/etheroll-whitepaper

Piasecki, P. J. (2016, December 21). Gaming Self-Contained Provably Fair Smart Contract Casinos. ResearchGate; https://www.researchgate.net/publication/311864045_Gaming_Self-Contained_Provably_Fair_Smart_Contract_Casinos

Dekking, M. (2005). A modern introduction to probability and statistics: understanding why and how. https://archive.org/details/modernintroducti00fmde

Yao, Kai; Gao, Jinwu (2016). "Law of Large Numbers for Uncertain Random Variables". IEEE Transactions on Fuzzy Systems. 24 (3): 615–621. doi:10.1109/TFUZZ.2015.2466080. ISSN 1063-6706. S2CID 2238905

Wikipedia Contributors. (2020, October 2). Probability theory. Wikipedia; Wikimedia Foundation. https://en.wikipedia.org/wiki/Probability_theory

Provable Documentation. (2015). Provable.Xyz. https://docs.provable.xyz/#background

Jamie Dimon Slams Bitcoin as a 'Fraud.' (2017, September 12). Bloomberg.com; Bloomberg. https://www.bloomberg.com/news/articles/2017-09-12/jpmorgan-s-ceo-says-he-d-fire-traders-who-bet-on-fraud-bitcoin

Martin, K. (2018, January 9). JPMorgan Chase CEO Jamie Dimon regrets saying Bitcoin is a "fraud". https://www.foxbusiness.com/markets/jpmorgan-chase-ceo-jamie-dimon-regrets-saying-bitcoin-is-a-fraud-but-still-isnt-interested-in-it

J.P. Morgan Creates Digital Coin for Payments. (2020). Jpmorgan.com. https://www.jpmorgan.com/solutions/cib/news/digital-coin-payments

PROJECT LINKS

1. The Arpa Games Dapp page, https://arpa.games/
2. Github code repository, https://github.com/arpacorp
3. Smart contract address, https://etherscan.io/address/0x76abdc570c37c8f9756b3506eafac501609177cc
4. Arpax ERC20 token address, https://etherscan.io/token/0x58c2A89Ff9522cF7f44C3B7b3C3DE2165eea9b5E

ACKNOWLEDGEMENT

The author would like to acknowledge the following people: Ma. Alma S. Fajardo, Arpacorp. Arpacorp Technical Team: Bernardo G. Parinas Jr. and Nino Paquito O. Pedida Jr. Aleck David S. Fajardo, Ateneo De Manila University. Andre Miras, The Etheroll Project. Carlos Mayorga, Smart Contract Development. Tracy Anne A. Navarro, Ateneo De Manila University. Eka Prasetyo P., User Interface Enhancement.

DOCUMENT CONTROL

11/25/2020 - v1.0. Initial Released.