How Truly Random Numbers, Cryptography and Blockchain Increases Trust In iGaming

GRAHAM LEACH

Visiting Lecturer, School of Design, Hong Kong Polytechnic University
Graham@Leach.com

Abstract

Games come in three flavors; Chance, Skill and Both. The outcomes of Games of Chance are driven by randomness. The outcomes of Games of Skill are driven by Player choice. The outcomes of Game of Both are driven by a combination of Chance and Skill. Distrust overshadows online gambling (iGaming) because Players suspect Operators of rigging games by subverting their randomness. A True Random Number Generator, Cryptography, and a Blockchain could mitigate this situation by enabling Operators to pre-publish game inputs prior to turns in such a way that Players could not defraud the Operators by using that information to influence their game play. In this paper, we discuss The BigBang Survival Run, an online variant of a parimutuel Game of Chance, where the above approaches are beginning to be implemented.

I. INTRODUCTION

iGaming first emerged on January 17, 1996 when the online gambling site Intertops accepted a USD50 bet from Jukka Honkavaara that favored Tottenham Hotspur over Hereford United. Mr. Honkavaara was also the first online gambling winner, getting his stake back plus a premium of USD2, for a grand total of USD52 (Casinoroom, 2018; Intertops, 2019). Since then, iGaming has become a major global industry that is projected to come within striking distance of USD74B by 2024, after having experienced a compound growth rate of 10% in the preceding decade (Hexa, 2019). But, while the future of iGaming looks bright from a revenue standpoint, a perennial cloud of distrust hangs over the industry. The root causes are myriad, but some of the primary drivers appear to be a lack of operational transparency on the part of iGaming Operators (Clarke, 2017), the innate hyper-sensitivity humans have to loss (Kahneman & Tversky, 1979) and the natural tendency for most people to want to shift blame instead of assuming responsibility for their own failings (Zuk, 1984).

II. THE SPECTRUM OF GAME TYPES

iGames come in three flavors. Games of Chance, where outcomes are determined entirely by randomness, lie at one end of the spectrum. Games of Skill, where outcomes are entirely dictated by Player choice, lie at the other end. Between the two is Games of Both, those games that feature a mixture of Chance and Skill (Figure 1).

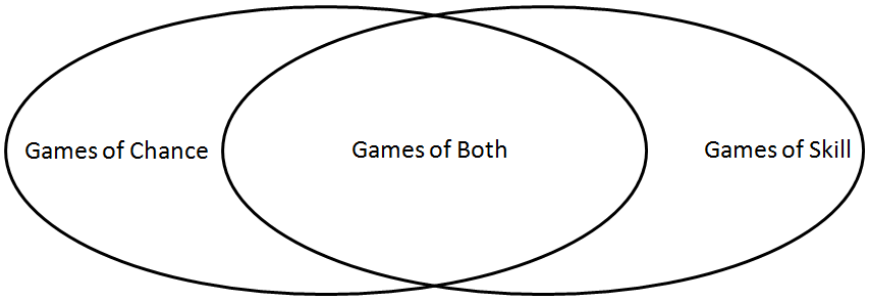

Figure 1: The Spectrum of Game Types

III. Game Type Examples

The following archetypes may help to further illustrate the differences between these types of games:

- The archetypical Game of Chance is "heads or tails", a coin-flipping game entirely dependent on randomness, where the outcome of any given turn cannot be influenced by any future turn, nor any of its prior turns, rendering it independent of Player choice.
- The archetypical Game of Skill is Chess, where each move encapsulates all of the information of each prior move, and which is in turn embeds all game information in the next move, making the game outcome dependent on Player choice and independent of randomness.
- There is no archetypical Game of Both because the Chance to Skill ratio varies so widely between examples of this type of game. Instead, it is presumed that any game featuring both Chance and Skill qualifies it as a Game of Both, a source of great confusion.

IV. Confusion Regarding Games of Both

A vague definition isn't the only reason why Games of Both is such a confused arena - Politics figure in too. In 1982, Backgammon was defined as a Game of Skill by a court in the USA (GamesColony, 2019), despite its obvious dependency on randomness (it uses the roll of two dice to generate turn-dependent information). The reason why it was classified as a Game of Skill appears to be mercy. The prosecuting jurisdiction (Oregon) arrested a Backgammon Competition Organizer for holding an amateur weekend Backgammon tournament featured an event entry fee and cash prizes. The presiding judge, no doubt wishing to avoid convicting an artless Backgammon hobbyist of a felony, opted instead to reclassify Backgammon as a Game of Skill. This example shows that Games of Both are also plagued by cultural, social and political factors, further muddying already unclear waters.

V. Wagering

iGaming is unabashedly about money. More specifically, it is about wagering money on a somehow uncertain outcome. Offering a rich universe of choice, iGaming offers a full gamut of game types (Chance, Skill, Both) in a huge amount of iterations and variations. For those who wish to play them, Games of Chance and Games of Both are fully represented. Even Games of Skill are accommodated in iGaming by way of an extremely comprehensive and sophisticated wagering ecosystem where bets may be placed on almost any event. This includes traditional scenarios such as races, boxing matches, and football games - but also exotic things like electoral results, weather, or even if a specific video gamer wins or loses a video game competition - a pursuit known as eSports (Takahashi, 2018).

VI. Losing

The main issue with people who place bets is that they usually lose. While most people understand that from an intellectual point of view, nobody enjoys the feeling of losing. This situation is further confounded by the fact that people are much more sensitive to losing than winning (Kahneman & Tversky, 1979), making the sting of loss even keener. Like anyone else who has failed, a punter who has just lost a wager is prone to seek an external reason for their failure other than bad decision-making powers. This helps them to explain away their loss and shift the responsibility for the negative outcome away, a very typical human response to failure (Zuk, 1984).

VII. Mutual Distrust, Accusations & Actual Cheating

Because the situation surrounding losing is already so fraught with psychological considerations, iGaming was bound to be overshadowed by distrust and suspicion on the part of Players, and a consequent adversarial relationship with Operators. Already pitted against each other by the dynamics of the ecosystem that they co-habitate, the situation is not improved when Operators fail to

be fully transparent about how the outcomes of their games are determined, particularly when putatively random numbers are driving those game outcomes. This has led to Players harboring nagging suspicions (or even voicing outright accusations) of Operators running "rigged" games whose randomness has been subverted (Cyborg PhotoshopVideos, 2017). Articles have been published featuring detailed explanations of how iGaming operators might go about cheating Players by subverting randomness (Stargame, 2018). iGaming-oriented chat boards teem with conflicting, often angry messages accusing a certain iGaming Operator, or even all iGaming Operators, to a certain degree of dishonesty when dealing with the randomness that both they and Players rely on to determine game outcomes (Casino Advisor, 2019).

VIII. True Random Number Generators

Random number generators falls into two broad categories: Pseudo-random and truly random. What distinguishes them is whether or not they are *deterministic*, which comes down to their input modality, or *seed*, along with the methodology by which that seed is manipulated. When it comes to pseudo-random number generators, a system-derived *seed* is typically used in conjunction with one of small number of accepted algorithms to generate something called a "relatively" random number (Singla, 2019). These numbers approach random, but are not truly random. True Random Number Generators, on the other hand, are generally specialized and hardware-oriented, and they use a wide variety of physical phenomena (Stipcevic, 2014) as a predicate for their outputs. True Random Number Generator hardware has been commoditized in recent years, and there now exists inexpensive dedicated integrated circuit True Random Number Generators costing less than USD5 on a unit volume basis (FDK, 2019) and even convenient USB stick format True Random Number Generators that can be purchased singly online for less than USD50 (BitBabbler, 2019; Moonbase-Otago, 2019).

IX. Cryptography

Cryptography is the practice and study of techniques that can be used to encode and transmit data in such a way that trusted parties may exchange information in circumstances where an unauthorized party may intercept those communication(s). Public Key Infrastructure (PKI), a subset of cryptography, utilizes a pair of keys (Public, Private) to sign, encrypt and decrypt information. Some aspects of PKI (encrypting information) can be a very computationally intensive process. Other aspects of PKI (validating information) is not that computationally intensive. One of the most useful applications of PKI is the *digital signature*, which can help to prove that a specific identity has created and signed the information in question, and in such a way that the receiver can validate that information in question has not been tampered with by a third party over space and/or time.

X. Blockchain

Blockchain (or Distributed Ledger Technologies) is a computer-based means of storing information in a highly secure and reliable way by embedding information in a set of data structures known as *blocks* which are then logically sequenced to form a *chain*. Blockchain tend to be implemented in a decentralized fashion, meaning that parallel copies of the resulting data structure is distributed geographically, which can increase availability and in some cases, performance. Because distributed databases suffer from latency and concurrency issues, which can negatively affect reliability and accuracy, blockchain databases use a range of *consensus* models to enable a best-effort representation of current reality, or the *world state*, with as high a level of fidelity as possible. Finally, blockchain databases are typically *append-only* data structures, which means information may only be added to them, giving them the valuable property of being *immutable* in terms of the information that has been committed to them.

XI. A Possible Technological Resolution To Mutual Distrust.

iGaming Operators have started to recognize that they must address Player mistrust. One way they can do this is to develop and deploy iGaming systems that integrate True Random Number Generators, Cryptography and Blockchain to increase transparency. In an ideal scenario, an iGaming operator would generate a random number using a True Random Number Generator, digitally sign it using PKI and then commit that result to a blockchain before turn of a Game of Chance or Game of Both begins. One the turn has concluded, any Player with a suspicion that the Operator had cheated them could verify the random number used to determine the turn outcome by accessing a public, persistent, immutable, time-stamped Blockchain transaction that contains the digitally signed random number used.

XII. Application: The BigBang Survival Run

The BigBang Survival Run is a variant of a *parimutuel game*, in which an arbitrary number of participants place a wager on a random event. With the BigBang Survival Run, a rocket ship traveling through space explodes once it has run out of fuel, but the amount of remaining fuel is unknown, making the time of the explosion impossible to predict. When the ship explodes, any passengers onboard are instantly killed. Those passengers who abandoned ship before the explosion survive and are rewarded, with those passengers who abandoned later receiving a larger reward.

XIII. Blockchain-Based Transactions

The BigBang Survival Run stores turn outcome information as a transaction on a blockchain to facilitate Player verification. An example transaction address appears below:

0xeaedec663efe5bd73778cc5e1c944afb78b8a3b9f38e66f5f918f90200032c60

Figure 2: Example BigBang Survival Run Blockchain Transaction Address

XIV. Transaction Verification

The BigBang Survival Run website features a convenient turn lookup feature, where the outcome of any turn may be retrieved by simply entering its transaction address. In the case of this turn, the ship traveled 2.079 units before it exploded, rewarding all players who left the ship prior to that event.

Figure 3: BigBang Survival Run Website Transaction Lookup Feature

XIII. Conclusions And Next Steps

Currently, The BigBang Survival Run features a single space-oriented game that logs only the outcome of any given turn. While this is a great start, the website could easily be extended to incorporate the mistrust-relieving measures that have been described in this paper.

Moreover, the possible universe of games that BigBang could deploy, via a synthesis of Truly Random Numbers, Cryptography and Blockchain, is truly vast. Each of these game categories holds literally millions of game variants - and the approach described in this paper could be equally applied to any them, neatly resolving the main issue that overshadows them all: The propensity of Players to seek for external reasons to blame their failures on others, which contributes to their mistrust of iGaming Operators. The approach described in this paper neatly addresses that issue, by equipping Players with a means to validate game inputs, rendering iGaming more transparent and verifiable in a way that is safe for both Players and Operators. This approach may also help to open the door to much wider adoption of iGaming by the general public, because - despite the persistent negative psychological and financial consequences of losing, Players will know it was due to "bad luck" rather than the possibility, however slight, that they may have somehow been cheated. This should enhance their perceived entertainment value, and heighten the iGaming entertainment experience.

XIV. Acknowledgements

I would like to thank BBGC for its gracious sponsorship of the Asia Pacific Blockchain Conference held in Singapore on June 01, 2019, where this paper was originally presented.

REFERENCES

BitBabbler.\2019. *BitBabbler: How to Get One*. Available: http://www.bitbabbler.org/buy.html [May 31, 2019].

CasinoAdvisor. 2019. *Do online casinos ever cheat players?* Available: http://www.casinoadvisor.com/forum/online-casinos/do-online-casinos-ever-cheat-players.html [May 31, 2019].

Casinoroom. 2018. *Inside the History of Online Gambling*. Available: https://www.casinoroom.com/blog/inside-the-history-of-online-gambling [May 30, 2019].

Cision. 2018. *Global Online Gambling Market Size Worth USD73.45 Billion by 2024: Hexa Research*. Available: https://www.prnewswire.com/news-releases/global-online-gambling-market-size-worth-usd-73-45-billion-by-2024-hexa-research-869794438.html [May 30, 2019].

Clarke, O. 2017. *Can blockchain technology improve online gambling transparency?* Available: https://www.osborneclarke.com/insights/can-blockchain-technology-improve-online-gambling-transparency [May 30, 2019].

Cyborg PhotoshopVideos. 2017. *Caught online Casino roulette cheat!! SCAM ALERT!! Please SHARE!* Available: https://www.youtube.com/watch?v=NN5a0-WBOxc [May 31 2019].

FDK. 2019. *True Random Number Generator (TRNG) RPG100/RPG100F*. Available: http://www.fdk.com/cyber-e/pi_ic_rpg100.html [May 31, 2019].

Fortune Palace, 2019. *Do online casinos cheat?*. Available: https://www.fortunepalace.co.uk/do-online-casinos-cheat.html [May 31, 2019].

Hexa. 2019. *Online Gambling Market Size and Forecast, By Type (Sports Betting, Casinos, Poker and Bingo), and Trend Analysis, 2014 - 2024*. Available: https://www.hexaresearch.com/research-report/online-gambling-market?utm-source=referral&utm-medium=prnewswire.com&utm-campaign=prn-5November-OnlineGambling-rd2 [May 30, 2019].

Intertops. 2019. *About Intertops*. Available: https://sports.intertops.eu/en/content/about [May 30, 2019].

Kahneman D. & Tversky A. 1979. *Prospect Theory: An Analysis of Decision under Risk*. Available: https://www.jstor.org/stable/1914185 [May 30, 2019].

Moonbase-Otago. 2019. *OneRNG External*. Available: https://moonbase-otago.myshopify.com [May 31, 2019].

Stargame, A. 2018. *How do online casinos cheat players?*. Available: https://medium.com/@alexstargame/how-do-online-casinos-cheat-players-25a835df75df [May 31, 2019].

Stipcevic, M. 2014. *True Random Numbers Generators*. Available: https://www.researchgate.net/publication/299824248_True_Random_Number_Generators [May 31, 2019].

Takahashi, D. 2018. *How esports, gambling, and sports betting are converging*. Available: https://venturebeat.com/2018/11/03/how-esports-gambling-and-sports-betting-are-converging [May 31, 2019].

Singla, Y. 2019. *Pseudo Random Number Generator (PRNG)*. Available: https://www.geeksforgeeks.org/pseudo-random-number-generator-prng [May 31, 2019].

Zuk, G. 1984. *On the Pathology of Blaming*. Available: https://link.springer.com/article/10.1007/BF00926927 [May 30, 2019].