

Probabilities around the Block: Analyzing Probability of Transaction Success for Various Blockchain Protocols*

James O'Malley

Tufts University, EE104 Fall 2023

Medford, Massachusetts

james.o_malley@tufts.edu

<https://github.com/jamesomalley/EE104>

December 12, 2022

Abstract: This paper analyzes the probability of a successful transaction occurring on a number of different blockchain protocols. Probability is measured over time to determine impact of major network upgrades on transaction success. It also explores the correlations between blockchain performance and price of the associated cryptocurrency tokens.

Keywords: blockchain, probability, bernoulli

*This paper is for informational purposes only. It is educational in nature and is not designed to be an offer or solicitation for the purchase or sale of any security, nor is it legal or tax advice. References to securities and strategies are for illustrative purposes only and do not constitute buy or sell recommendations. The information in this report should not be used as the basis for any investment decisions. At time of publishing, author held financial interest in Ethereum (ETH) and Polygon (MATIC) .

1 Introduction

Though their associated cryptocurrency tokens are known by investors for volatile swings in price, the blockchain technology underlying these assets is intended to perform consistently regardless of price fluctuations [1]. A blockchain is a database of transactions that is updated and shared across many computers in a network [2]. An in-depth discussion of blockchain technology is outside the scope of this paper, however, blockchains generally allow users to transact on a publicly available ledger to transfer digital assets, execute smart contracts, or store data [2]. The Bitcoin blockchain is arguably the first and most popular blockchain, however, many competitive technologies, such as Ethereum, Solana and Avalanche, have arisen since the publication of the initial Bitcoin white paper in 2008 [3].

Researchers have explored the probabilistic nature of blockchains from a number of different angles, including the probabilistic conditions of achieving consensus on a blockchain, risk assessment using a blockchain protocol, network security using a probabilistic model, and even a new method for validating transactions ("proof-of-probability") [5][6][7][8]. This paper will extend this research by comparing the probability of a successful transaction occurring across different blockchain protocols – Bitcoin, Ethereum, Polygon, Solana, and Avalanche – using data available from the protocols' public ledgers.

While the exact mechanics of specific blockchain technologies vary by network, transactions on a blockchain are verified by other network participants and will succeed or fail for a variety of reasons. For example, transactions on the Ethereum network can fail due to too low of computational cost allocated to the transaction by the user (referred to as "out of gas"), the transaction was reverted by one of the transaction's counterparties, bad instructions within the smart contract executing the transaction, or a token transfer failure (e.g. insufficient balance) [4].

This paper aims to compare the performance of various blockchain protocols by developing a model for the probability of transaction success and exploring statistical relationships between transaction success and asset price. It will begin by establishing a scope of analysis to identify which blockchain protocols are included in the analysis and how data is gathered. The next section will describe how probability can be applied to understanding blockchain transaction success. The remainder of the research will compare the probability of transaction success across the blockchain protocols in scope and measure the correlation between transaction success and the price of the cryptocurrency tokens associated with each blockchain.

2 Analysis Scope

The blockchains included in this research are listed in Table 2.1 below. Table 2.1 includes several metrics intended to measure the popularity of each blockchain:

- Market capitalization: the total USD (\$) value of all tokens on the blockchain [12]
- Active addresses: number of unique addresses involved in a successful transaction as of November 30, 2022 [13]

- Transactions: how many unique transactions (n) were included in probability calculations

Table 2.1

Name	Token	Market Cap[10]	Active Addresses[13][14][15]	Transactions[11]
Bitcoin	BTC	\$327.5B	820K	773M
Ethereum	ETH	\$15B	374K	1.8B
Solana	SOL	\$5.1B	577K	26B
Avalanche	AVAX	\$4.2B	38K	208M
Polygon	MATIC	\$7.9B	3K	2.3B

Transaction data was accessed using Dune Analytics for Ethereum, Solana, Avalanche and Polygon blockchains and Statoshi.info for Bitcoin [11][15]. Dune Analytics aggregates raw blockchain transaction data and stores it in a SQL accessible table for querying. Statoshi.info provides an interactive web application of Bitcoin transactions, including whether a transaction was accepted or rejected.

While the date of the earliest transaction included in the analysis varies based on blockchain, all transaction data is through November 30, 2022.

More specifics of the underlying data collection and aggregation of this research paper, including the queries and datasets, can be found at [here](#).

3 Applying Probability to Blockchain Transactions

To help understand how probability applies to blockchain transactions, there are a few areas in which it helps to define equations which will be used in this research:

- The probability ($P[S]$) of a given transaction's success ($s=1$) or failure ($s=0$)
- Establishing an equation for calculating p for each blockchain in totality and over time
- Measuring the correlation between blockchain transaction success/failure, total market capitalization and token price

For a given transaction, the probability of a success (S) is a Bernoulli (p) random variable. Bernoulli random variables apply to sequential experiments with independent trials in which each subexperiment has two possible outcomes[12]. Each attempted transaction can be considered a Bernoulli trial for which there is only two possible outcomes: success ($s=1$) or failure ($s=0$).

As a Bernoulli random variable, the probability mass function (PMF) of a successful blockchain transaction can be expressed as:

$$P_S(s) = \begin{cases} 1 - p & s = 0 \\ p & s = 1 \\ 0 & \text{otherwise} \end{cases}$$

where the parameter p is in the range of $0 < p < 1$ [12].

To calculate p for each individual blockchain transaction, t = number of total successful transactions and n = number of total attempted transactions. $p = P[S] = \frac{t}{n}$.

It is possible the probability of a successful transaction changes over time due to market fixes and technological changes such as an influx of new users more likely to make errors or upgrades to the blockchain technology by developers. As such, the probability of a successful transaction for any given month is $P[S_i] = \frac{t_i}{n_i}$ where i denotes the month included in calculations.

For the purposes of this research, the reliability of a blockchain will be measured by the expected value $E[S]$ (those with a higher $E[S]$ will be considered higher performing), and $Var[S]$ will be used to evaluate performance consistency. Expected value of S is $E[S] = \mu_S = \sum sP(s)$. Variance is calculated as $Var[S] = \sigma^2 = E[(S - \mu_S)^2]$.

The tokens associated with blockchain technologies (e.g. BTC for Bitcoin) are considered significant investment vehicles and, as such, it may be useful to understand whether a correlation exists between the performance of the underlying blockchain (i.e. probability of transaction success/failure) and the USD price of the associated token. The correlation coefficient is a normalized version of covariance that indicates the relationship of two random variables regardless of measurement units [12]. In this instance, the probability of a successful transaction (S) will be measured as a percentage and token price (X) will be measured in USD.

The correlation coefficient of these two random variables X and S is:

$$\rho_{X,S} = \frac{Cov[X,S]}{\sqrt{Var[X]Var[Y]}} = \frac{Cov[X,S]}{\sigma_X \sigma_S}$$

To calculate the covariance between asset price and the probability of transaction success, $Cov[X,S] = E[(X - \mu_X)(S - \mu_S)]$ [12].

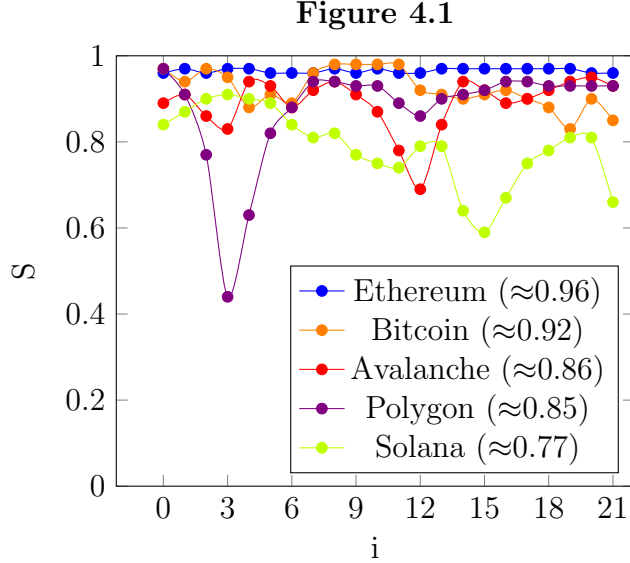
4 Comparison of Blockchain Transaction Success Probabilities

To analyze the probability of a successful transaction on each blockchain in scope of this research ($P[S]$), individual blockchain transactions were queried using Statoshi.info (Bitcoin) and Dune Analytics (all other blockchains) to measure values for t and n in order to calculate $P[S]$. The results of this analysis can be found in Table 4.1 below.

Table 4.1

Name	Date Range	t	n	p	$1-p$
Ethereum	10/1/17-11/30/22	1,681,731,602	1,736,720,621	0.968851	0.031149
Bitcoin	12/1/17-11/30/22	677,235,000	773,491,045	0.88	0.12
Avalanche	2/1/21-11/30/22	178,690,015	207,922,514	0.859623	0.140377
Polygon	6/1/20-11/30/22	1,927,375,364	2,252,925,245	0.855499031	0.144500969
Solana	10/1/20-11/30/22	20,754,207,378	26,561,603,366	0.781361241	0.218638759

From Table 4.1, it is observed that a transaction on the Ethereum blockchain has the greatest probability of success (0.968851) while a transaction on the Solana blockchain has the lowest success probability (0.781361241). The blockchain industry is fast moving, however, and results may change over time as upgrades are made to the underlying technology or new users are onboarded to the networks. Figure 4.1 shows the value of $P[S]$ on a monthly basis since February 2021 (the earliest month for which data is available for all blockchains). $i = 0$ for February 2021, $i = 1$ for March 2021, etc.



As indicated in Figure 4.1, the probability of transaction success for each blockchain does vary month-to-month and considering only more recent transactions does have some impact on results. Ethereum is both the best performing blockchain (with the highest $E[S] = 0.97$) and the most consistently performing blockchain with a variance (σ^2) of ≈ 0.002 . In contrast, Solana is the lowest performing blockchain overall with an $E[S] = 0.79$ but is more consistent than Polygon with a variance of $\approx .0077$ vs Polygon's variance of ≈ 0.0149 .

Polygon's higher variance appears to be a result of degraded performance from April to June 2021 which coincides with the onboarding of major decentralized finance protocols which may have influenced performance either due to new technology or new functionality [18].

Bitcoin's transaction success probability had the greatest change when considering only the more recent timeframes as depicted in Figure 4.1. The overall transaction success probability as measured in Table 4.1 is $p = 0.88$, however, $p = 0.96$ in the shorter timeframe. A major upgrade to the network, Taproot, went live in November 2021 and may have had positive impact on the transaction probability success [19].

5 Correlation Between Transaction Success and Asset Price

In section 4, the probability of a successful blockchain transaction was established for each of the blockchains included in this research, including a month-over-month calculation of $E[S]$. Many investors consider the cryptocurrency tokens associated with each blockchain technology as an investment asset class separate from stock markets, real estate and other traditional financial assets. A logical hypothesis is that a correlation exists between the performance of the blockchain technology and the value of its associated tokens.

Table 5.1 provides results of the the correlation coefficient of month-to-month $P[S]$ results and the closing price of the associated assets (the price on the last day of the month).

Table 5.1

Name	$E[S]$	$E[X][20]$	$Cov[X, S]$	ρ
Ethereum/ETH	0.96	\$2,487.79	1.66	≈ 0.374
Bitcoin/BTC	0.92	\$38,562.95	231.67	≈ 0.395
Avalanche/AVAX	0.86	\$44.25	-0.84	-.40268
Polygon/MATIC	0.85	\$1.17	-0.02	-0.28673
Solana/SOL	0.77	\$75.08	-0.38	-0.07

The results reflected in Table 5.1 appear to suggest that a correlation does not exist between the probability of blockchain transaction success and the prices of their associated cryptocurrency tokens. This suggests that the value investors place on the cryptocurrency tokens are associated with another market factor than transaction success of the underlying technology.

The calculated values for ρ are never strong enough to suggest a relationship either postively or negatively ($\pm .75$) and do not agree in direction. Bitcoin and Ethereum have a moderately positive correlation between price and the probability of transaction success while the others are negative.

6 Conclusion

This research established an approach for analyzing the probability of a successful transaction on the Avalanche, Bitcoin, Ethereum, Solana and Polygon blockchains as well as a method to correlate that probability to the prices of their associated cryptocurrency assets.

The analysis observed that difference do exist between each blockchain technology in terms of the probability that a given transaction will be successful, and that probability fluctuates over time. Significant changes in the probability of transaction success appear to coincide with major development milestones of the technology.

The analysis also measured whether a correlation exists between the probability of a transaction success and the price of cryptocurrency tokens. The results indicated that there is not a correlation between the two, and investors value the cryptocurrency tokens on other factors.

Blockchain technology represent a new method for peer-to-peer transactions on a public ledger. The wealth of data that these protocols generate provide ample opportunities for future research into users transact with each other.

7 Reference

1. Tyler Cowen. "Crypto's Values Comes From Crypto's Volatility." Bloomberg.com. <https://www.bloomberg.com/opinion/articles/2022-06-02/how-should-we-value-crypto-by-how-volatile-crypto-assets-are>, June 2, 2022 (accessed December 3, 2022)
2. Ethereum Foundation. "What Is Ethereum? — ethereum.org" Ethereum.org. <https://ethereum.org/en/what-is-ethereum/> (accessed December 3, 2022).
3. Vinay Gupta. "A Brief History of Blockchain". Harvard Business Review. <https://hbr.org/2017/02/a-brief-history-of-blockchain> (access December 3, 2022).
4. Kaven Choi. "What are the Reasons for Failed Transactions?" Etherscan.io. <https://info.etherscan.com/reason-for-failed-transaction/> (accessed December 3, 2022).
5. Markinovic et al. "Probabilistic Consensus of the Blockchain Protocol". https://home.inf.unibe.ch/~tstuder/papers/20190614_probability_blockchain.pdf
6. T. Salman, R. Jain and L. Gupta, "Probabilistic Blockchains: A Blockchain Paradigm for Collaborative Decision-Making," 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2018, pp. 457-465, doi: 10.1109/UEMCON.2018.8796512.
7. K. Aiyar, M. N. Halgamuge and A. Mohammad, "Probability Distribution Model to Analyze the Trade-off between Scalability and Security of Sharding-Based Blockchain Networks," 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), 2021, pp. 1-6, doi: 10.1109/CCNC49032.2021.9369563.
8. Kim, Sungmin & Kim, Joongheon. (2018). POSTER: Mining with Proof-of-Probability in Blockchain. 841-843. 10.1145/3196494.3201592.
9. Shijie Zhang, Jong-Hyouk Lee, Analysis of the main consensus protocols of blockchain, ICT Express, Volume 6, Issue 2, 2020, Pages 93-97, ISSN 2405-9595, <https://doi.org/10.1016/j.ict.2019.08.001>. (<https://www.sciencedirect.com/science/article/pii/S240595951930164X>)
10. CoinMarketCap, "Cryptocurrency Prices, Charts And Market Capitalizations — CoinMarketCap." <https://coinmarketcap.com/> (accessed December 8, 2022).
11. Dune Analytics AS. "Dune." Dune. <https://dune.com/queries> (accessed November, 2022)
12. Yates, Roy D., and David J. Goodman. *Probability and Stochastic Processes: a Friendly Introduction for Electrical and Computer Engineers*. Third edition., John Wiley & Sons, 2014.
13. DST Systems, Inc. "Understanding Market Capitalization". <https://www.fidelity.com/learning-center/trading-investing/fundamental-analysis/understanding-market-capitalization> (accessed December 3, 2022).

14. Glassnode. "Bitcoin: Active Addresses". <https://studio.glassnode.com/metrics?a=BTC&m=addresses.ActiveCount> (accessed December 8, 2022).
15. Statoshi.info. "Transactions - Grafana." <https://statoshi.info/d/0000000006/transactions?orgId=1&from=now%2Fy&to=now> (accessed December 8, 2022).
16. Solscan. "Solana Analytics — Solscan." <https://analytics.solscan.io/> (accessed December 8, 2022).
17. Avalanche. "Avalanche (C-Chain)." https://subnets.avax.network/c-chain/stats?timespan999=ONE_YEAR (accessed December 8, 2022).
18. Polygon. "About Us — Polygon." <https://polygon.technology/about> (accessed December 12, 2022).
19. Bitcoin.org. "Bitcoin Core 0.21.1 released" <https://bitcoin.org/en/releases/0.21.1/> (accessed December 12, 2022).
20. Yahoo. "Yahoo Finance - Stock Market Live, Quotes, Business & Finance News" <https://finance.yahoo.com/> (accessed December 12, 2022).