Stochastic analysis of the success rate in atomic swaps between blockchains

Bence Ladóczki, József Bíró, János Tapolcai
ELKH-BME Future Internet Research Group and ELKH-BME Information Systems Research Group,
Department of Telecommunication and Media Informatics, Faculty of Electrical Engineering and Informatics (VIK),
Budapest University of Technology and Economics (BME), {ladoczki,biro,tapolcai}@tmit.bme.hu

***Abstract*—The classical way to exchange digital assets is to use a centralized exchange, which goes against one of the main organizing principles of crypto currencies, namely the decentralized property. There has been an increased interest in finding alternative solutions to eliminate the need for these centralized crypto currency exchanges. Atomic swaps enable digital asset holders to exchange their tokens without intermediaries. Setting aside the risk associated with the centralized exchange, converting between digital assets on these platforms is very convenient and attracts users in massive quantities. Once a sell (or buy) order is placed and accepted by the platform and a matching buy (or sell) order is found there is no way to waive the commitment and the order is executed no matter what. The situation is altered when one uses atomic swaps, due to the nature of the atomic processes. If a party can abandon the deal at certain stages the atomic swap becomes an option. These options have been extensively studied in the past with various models to simulate the changes in the underlying stock. In the current work, we simulate strategic behaviors on historical market data, analyse crypto currency atomic swaps using the Merton Jump Diffusion model and propose a theoretical solution to increase the success rates in atomic swaps. The aim of this analysis is not forecasting, but rather a more accurate description of the optionality in atomic swaps.**

I. Introduction

With the advent of blockchain based technologies and crypto currencies there is an increased interest in decentralized systems. The developers of the first crypto currency, Bitcoin [1] and many of their aftercomers tout the importance of decentralization in crypto currency networks. Solid research has indeed shown that many of these systems become unstable once there is an entity that has control over the majority. However, when users are trying to exchange their digital assets with each other they usually perform this on a centralized cryptocurrency exchange. The fact that the exchange itself stores private keys and as a result operators can steal funds,[1] whenever they wish to do so is very concerning. The storage of private keys is not the only source of vulnerability when it comes to centralized exchanges. Getting hold of a substantial amount of cryptocurrency stake by operating a centralized exchange is much easier compared to proof-of-work (PoW) mining or proof-of-spacetime [2] farming as hoarding and operating a large number of PoW miners or farming HDDs is not a straightforward thing to do. Consequently, these exchanges pose risk to PoS currencies and from a user perspective, tedious KYC (know-your-customer) processes preclude a wider adoption of blockchain technologies. Also, exchanging digital assets on centralized exchanges incurs an exchange fee which can be thought of as money that is paid in exchange for a guarantee that the transaction takes place with a probability equal to 1. Solutions that enable users to exchange digital assets in a decentralized manner kill more birds with one stone. In the early days, decentralized exchanges (DEx) were developed to act as matchmakers between the parties rather than actually registering private keys.

One step further, if one desires true decentralization, low trading fees and peer-to-peer deals between inhomogeneous blockchain networks without third-party arbitration the matchmaker based implementation can be replaced by atomic swaps. The atomic property implies that none of the parties is worse off in any of the stages of the exchange [3]. Atomic swaps can be realized using Hash Time Locked Contracts (HTLCs)[2] if the chain implements contract functionalities and adaptor signatures can be used for the same purpose with group homomorphism based signature schemes. The swap takes place only if parties cooperate and there is no dishonest party intentionally intercepting the process. Therefore, atomic swaps are inherently accompanied by a tradeoff, namely that while fees are lowered, there is a non-zero probability of failure during the deal. In addition to intentional misbehavior atomic swaps might fail to succeed if one of the parties goes offline. There could be several reasons for a party to become unresponsive and in such situations, the coins initially locked into the swap get refunded to their original owners. Clearly, this constitutes a call option for one party and a put option for the other. An implementation in this primitive form without a risk premium can become unstable as there is no incentive for the parties to stay in the swap if the exchange rate moves in an unfavourable direction.

Option pricing has extensive literature and foretelling stock prices is one of the key areas of quantitative finance theories. The Black-Scholes (BS) formula for option pricing [4]

This work was supported in part by Project no. 124171 and 128062 that have been implemented with the support provided by the National Research, Development and Innovation Fund of Hungary, financed under the K_17 and K_18 funding schemes, respectively.

[1] https://en.wikipedia.org/wiki/Mt._Gox

[2] https://en.bitcoin.it/wiki/Hash_Time_Locked_Contracts

assumes that stock prices are governed by a drift and a Geometric Brownian Motion (GBM) component. The expectation value of the stock price, the probability density function (PDF) and the cumulative density function (CDF) can be expressed in a relatively simple form and a game theoretical analysis of atomic swaps was performed in [5] using these formulas. Although the solution of the BS differential equation can be used to describe the principal component of the movements in the stock price it fails to describe the jumps that occur on exchanges due to the arrival of information that triggers crashes and rallies. These jumps are incorporated in the Merton Jump Diffusion (MJD) [6] model by extending the drift in the GBM with a jump term.

Our paper is organized as follows. Firstly, we derive the necessary formulas to express the expected value of the price, the PDF and the CDF for the MJD model, then we give a short recap on how signature schemes work. Then, we describe how atomic swaps can be implemented and examine the behavior of atomic crypto currency swaps using the MJD model. Finally, we take historical exchange rates and simulate the actual strategic games for each party and also provide numerical results to shed light on the success rate of the swaps.

II. Related Work

The feasibility of atomic swaps and their vulnerabilities are being actively researched. Readers interested in a general overview of decentralized exchanges, blockchain technologies and atomic swap projects should refer to [7], [8] and [9]. The authors of [10] give a proposal for a protocol that would incentivize miners to confiscate funds of misbehaving participants to improve the security of HTLCs. In [11] the authors go even further and they propose atomic crosschain transactions for Ethereum private sidechains that can be implemented without HTLCs. Packetized payments [12] provide a promising solution for cross-ledger transactions in adversarial environments. Atomic swaps can also be implemented using homomorphic hashing [13]. Details on how to specify and check smart contract models for on-chain and cross-chain atomic swaps are given in [14]. Readers can find a detailed analysis in [15] on the importance of strongly connected directed graphs in cross-chain swap protocols.

Game theory has been applied several times to analyze the utility of atomic swap participants. In [16] and [17] for example, the authors present a complete framework to analyze multiple asset exchanges between different chains as strategic games. The essence of the problem is discussed in detail in [18] where atomic swaps are treated as premium-free American Call Options and simulated using the notorious Cox-Ross-Rubinstein model [19]. [20] analyzes crypto currencies from a financial point of view and propose inflation control mechanisms which might have important implications in the future as far as price dynamics are concerned. Mitigations to a few existing problems in atomic swaps are given in [21] to open up new means for derivative trading on existing crypto currencies using atomic swaptions. Geometric Brownian motion has been applied to simulate the behavior of atomic swaps for real-world currency pairs [22]. The current work is different from all of the above mentioned because we analyze the swaps using the Merton Jump Diffusion model. To the best of our knowledge, no such analysis has been carried out and reported in the past.

III. Price dynamics

The solution to the BS model describes the stochastic stock price P_t at time t as follows:

$$P_0 e^{\left(\mu-\frac{\sigma^2}{2}\right)t+\sigma W_t} \tag{1}$$

with μ denoting the drift and W_t the Wiener process component. The expectation value, the PDF and the CDF of the price can be expressed as:

$$\varepsilon^{BS}(P_t,\tau) := \mathbb{E}^{BS}(P_{t+\tau}|P_t) = P_t e^{\mu\tau} \tag{2}$$

$$\mathbb{P}^{BS}[P_{t+\tau}=x|P_t] = \frac{e^{-\frac{(\ln(\frac{x}{P_t})-(\mu-\frac{\sigma^2}{2})\tau)^2}{2\tau\sigma^2}}}{\sqrt{2\pi\tau}\sigma x} \tag{3}$$

$$C^{BS}(x,P_t,\tau) := \mathbb{P}^{BS}[P_{t+\tau}\leq x|P_t] = \frac{\operatorname{erfc}(-\frac{\ln(\frac{x}{P_t})-(\mu-\frac{\sigma^2}{2})\tau}{\sqrt{2\tau}\sigma})}{2} \tag{4}$$

The Merton Jump Diffusion model extends the BS model with a compound Poisson process ($\sum_{i=0}^{N_t} Q_i$) and the stochastic price becomes:

$$P_t^{MJD} = P_0 exp\{(\mu-\frac{\sigma^2}{2})t + \sigma W_t \ + \sum_{i=0}^{N_t} Q_i\} \tag{5}$$

In the MJD model, the number of jumps N_t is a Poisson process with rate λ, and the jump sizes Q_i are i.i.d. random variables (also independent from N_t) and described by a common normal distribution with parameters μ_j and σ_j (the index j stands for jumps). Along with equations (3) and (4), the PDF of the asset price in the MJD model can be expressed as a weighted sum of normal densities:

$$P^{MJD}(x,P_t,\tau) := \mathbb{P}^{MJD}[P_{t+\tau}=x|P_t] =$$

$$e^{-\lambda\tau}\textstyle\sum_{k=0}^{\infty}\frac{(\lambda\tau)^k}{k!}\frac{1}{\sqrt{2\pi}(\sqrt{k}\sigma_j+\sqrt{\tau}\sigma)}\frac{e^{-\frac{1}{2}\left(\frac{\ln(\frac{x}{P_t})-k\mu_j-(\mu-\frac{\sigma^2}{2})\tau}{\sqrt{k}\sigma_j+\sqrt{\tau}\sigma}\right)^2}}{x}\ , \tag{6}$$

and we derive the CDF of the MJD model as:

$$C^{MJD}(x,P_t,\tau) := \mathbb{P}^{MJD}[P_{t+\tau}\leq x|P_t] =$$

$$e^{-\lambda\tau}\sum_{k=0}^{\infty}\frac{(\lambda\tau)^k}{k!}\frac{\operatorname{erfc}(-\frac{\ln(\frac{x}{P_t})-k\mu_j-(\mu-\frac{\sigma^2}{2})\tau}{\sqrt{2}(\sqrt{k}\sigma_j+\sqrt{\tau}\sigma)})}{2}\ . \tag{7}$$

And finally, using the generating function approach the expected value of the price in the MJD model can be expressed as:

$$\varepsilon^{MJD}(P_t,\tau) := \mathbb{E}^{MJD}(P_{t+\tau}|P_t) = P_t e^{\mu\tau} e^{\lambda\tau(e^{\mu_j+\frac{\sigma_j^2}{2}}-1)} \tag{8}$$

These are the formulas that will be used in the following game theoretical analysis, with the infinite summations above truncated at k_{max}. As crashes and rallies are frequent on crypto currency markets, presumably, the MJD model gives a more accurate description of the underlying problem.

IV. Atomic swaps

The ownership of a digital asset in blockchain networks is equivalent to knowing a solution to an NP-hard problem that is computationally infeasible to break. In essence, a transaction is nothing more than proving that the buyer possesses some kind of secret (verification step) without divulging anything useful about the secret (zero-knowledge). In atomic swaps, however, in addition to these, the parties should also exchange these secrets (exchange step). These two goals are a bit controversial because the buyer has to prove and then reveal his secrets. The fact that any NP statement can be proved in zero-knowledge [23], and consequently that any NP-hard problem can be used for this purpose further complicates the interpretation of atomic swaps. The most widely adapted NP-hard problem is the discrete logarithm problem in a prime field used to generate public-private key pairs and prove that a certain user possesses a digital proof of a claim that is hard to break as long as the intractability of the discrete logarithm assumption holds. Moreover, modular exponentiation, by the law of exponents is a homomorphism. This favourable property makes the discrete logarithm problem a convenient and ubiquitous tool both for privacy conserving implementations [24] and blockchains.

Using a more practical narrative, atomic swaps provide means to exchange tokens between two independent chains without going through a centralised crypto currency exchange. In a blockchain network, users submit transactions to nodes in the form of messages. These messages are signed and the signatures serve as proofs to claims to show that a user can invert the exponentiation in the chosen prime field. Subsequently, nodes can check the validity of these messages by validating the signature. Elliptic Curve Digital Signature Algorithm (ECDSA) is among the most popular schemes to augment messages with user signatures in crypto currency networks, for example Bitcoin uses the `secp256k1`[3] curve for signature generation and SHA256 hashes for authenticating transactions. Signatures generated by multiple users (multisig) are easy to implement if the signature scheme is additive, in other words the sum of the public keys can be used to validate a multisig. With this in perspective, the BIP-340 proposal in the bitcoin network introduces Schnorr [25] signatures over the `secp256k1` elliptic curve. The additive property further enables the signers to offset their signatures and an atomic swap can be implemented using these partial signatures. In order to ensure that none of the parties ends up worse off (due to malicious behavior for example) the assets are transferred to a multisig output address that can only be spent by a 2-to-2 multisignature. Once a party spends one of the outputs, the offset gets revealed and the other party learns the secret that is necessary to unlock the coins on the other chain.

Atomic swap implementations usually rely on complex scripting logic or smart contract functionality [26]. While one implementation can be used between two certain chains it might not work between two other chains due to the nature of the signature schemes and other chain specific peculiarities. Details of an actual implementation to realize atomic swaps between Monero and Bitcoin are given in [27] and the actual software has gone live recently[4]. The subtlety of this proposal lies in the fact that Monero uses `edward25519` and Bitcoin uses `secp256k1` groups to generate public-private key pairs. In order to find a common divisor between the two chains, the parties have to exchange proofs to prove that they share a common discrete logarithm across their respective groups. During the execution of the protocol one-time Verifiably Encrypted Signatures (VES) [28] are exchanged and in the final stage, the secret decryption key that is required to sign the last transaction is extracted from the decrypted signature and the recovery key. For the sake of simplicity, we chose to analyze atomic swaps implemented using adaptor signatures where the final signature is obtained by simply subtracting the published signature by the other party to obtain the signature offset.

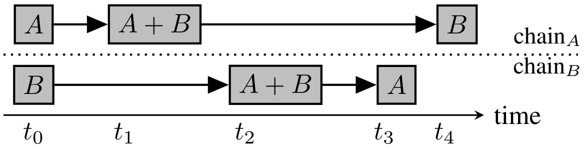

Figure 1: The timeline of an atomic swap

V. Game Theoretical Analysis of Atomic Swap

The atomic swap protocol to exchange digital assets between two independent blockchains based on Schnorr signatures consists of the following steps (see also Figure 1):

- t_0: the parties agree on the exchange rate P^* and other conditions
- t_1: A locks the agreed amount of token$_a$ on chain$_A$
- t_2: when B learns that A has locked token$_a$ on chain$_A$ he locks the agreed amount of token$_b$ on chain$_B$
- t_3: A unlocks token$_b$ on chain$_B$ and reveals the signature offset
- t_4: with the signature offset B can now unlock token$_a$ on chain$_A$ and receives it at t_5

From a game theoretical perspective, t_3 is the first point in time worth investigating as B does not alter the outcome of the swap by not unlocking the tokens at t_4. At t_3 A will choose between unlocking and aborting based on the expected value of the tokens. Similarly, t_2 and t_1 are points in time in which the parties can influence the outcome of the swap. At each point, one can express the utility of each party based on P^* and other conditions. For a detailed derivation of these quantities, refer to [5]. Here we are interested in the success rate of the swap when the BS model is replaced by the MJD model. The cut-off price at t_3 is expressed as:

$$P_{t_3}(P^*) = \frac{P^* e^{r_a \tau_b}}{(1+\alpha_a) e^{r_a(\varepsilon_b + 2\tau_a)}} \frac{1}{e^{\mu \tau_b} e^{\lambda \tau_b (e^{\mu_j + \frac{\sigma_j^2}{2}} - 1)}} \tag{9}$$

[3] https://en.bitcoin.it/wiki/secp256k1

[4] https://www.getmonero.org/2021/08/20/atomic-swaps.html

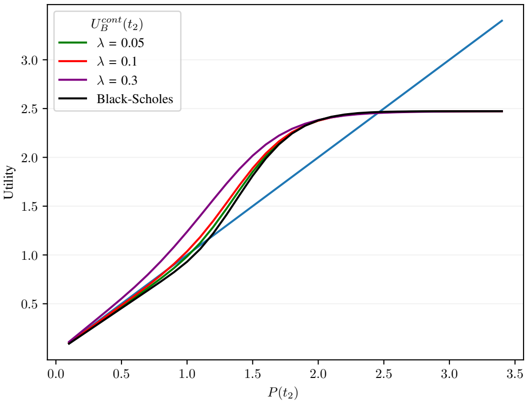

Figure 2: Party B's utility at time t_2 with MJD and BS. The following parameters were used for this calculation: P^* = 2.4, σ = 0.1, μ = 0.002, τ_a = 3, τ_b = 4, $\alpha_a = 0.3$, $\varepsilon_a = 1$, $\varepsilon_b = 1$, $r_a = 0.01$, $r_b = 0.01$, $P_{t_0} = 2$, $\mu_{MJD} = 0.01$, $\sigma_{MJD} = 0.1$, $k_{max} = 20$.

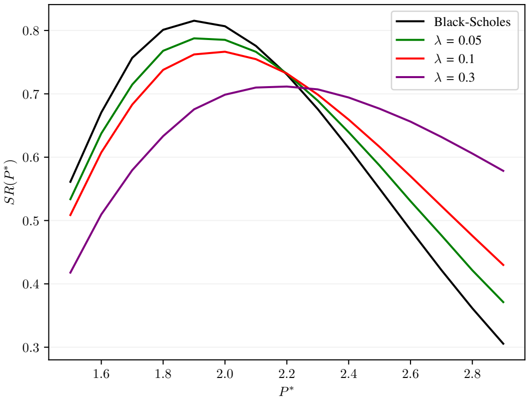

Figure 3: Jump intensity vs. success rate of the atomic swap with MJD and BS. σ = 0.1, μ = 0.002, τ_a = 3, τ_b = 4, α_a = 0.3, ε_a = 1, ε_b = 1, r_a = 0.01, r_b = 0.01, P_{t_0} = 2, $\mu_{MJD} = 0.01$, $\sigma_{MJD} = 0.1$, $k_{max} = 20$.

The success rate of the atomic swap assuming that A has made her initial move in t_1 is expressed with the following integral:

$$SR(P^*) = \int_{\underline{P_{t_2}}(P^*)}^{\overline{P_{t_2}}(P^*)} P^{MJD}(x, P_{t_1}, \tau_a)[1 - C^{MJD}(P_{t_3}(P^*), x, \tau_b)]dx \;, \tag{10}$$

where the lower and the upper limits of the integration are numerically determined by finding a feasible range in which the utility of party B is greater in value in case he chooses to continue the deal. Now we are in a position to compare the utility of each party at t_1, t_2 and t_3 and to calculate $SR(P^*)$ using the MJD model.

VI. Numerical results

The cut-off price at t_3 is a linear function of the agreed price (P^*) according to (9) and this formula is used to calculate the utility of party B when he chooses to proceed at t_2. Numerical results for $U_B^{cont}(t_2)$ are presented on Figure 2. for the BS model and for the MJD model with different jump intensities (λ). For low P$_{t_2}$ values B's utility increases with λ as the probability of P$_{t_3}$ $<$ P$_{t_2}$ decreases when there is more chance for a positive price jump (note that μ_{MJD} is positive). The BS curve was calculated with the MJD equations with $\mu_{MJD} \to 0$, $\sigma_{MJD} \to 0$ and $\lambda \to 0$. On Figure 3. we present $SR(P^*)$ values calculated with different jump intensities and with the BS model.

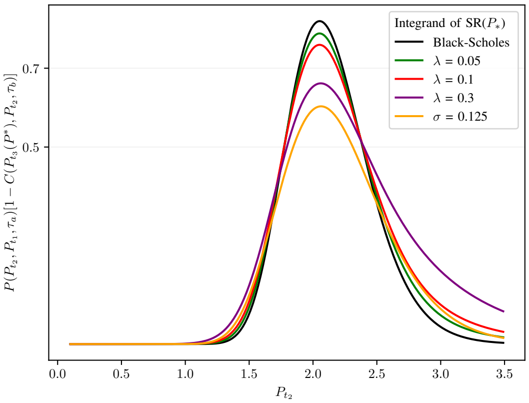

Figure 4: The integrand of $SR(P_*)$ vs. jump intensity for P_* = 2.4. The line σ = 0.125 refers to a BS model with no jump process.

From Figure 3. we can conclude that higher jump intensity in the MJD process decreases the rate of success. In order to understand the connection between λ and $SR(P_*)$ we found it expedient to plot the integrand of the success rate in Figure 4. Clearly as $\lambda \to 0$ the MJD model approaches the BS model and the success rate increases with the decreasing likelihood of jumps. These unexpected jumps in the exchange rate can render the atomic swap unsuccessful as the utility maximizing parties choose to abort the deal once the exchange rate enters a non-feasible range. We found that for intensities where the MJD probability density is smaller than the BS density the success rate decreases. The authors in [5] observed that $SR(P_*)$ decreases rapidly with increasing σ. Intuitively large deviations in the price can be treated as jumps. Therefore we conjectured that increasing σ in the BS model would lead to the same effect as switching the jumps on. This assumption has been numerically validated in Figure 4. from which we can deduce that increasing σ from 0.1 to 0.125 produces a similar effect in the success rate as incorporating an MJD process with $\lambda = 0.3$.

Next, we turn our attention to real-world data. In order to obtain approximate exchange rates, we subscribe to web socket streams using an API provided by Binance[5]. Our goal was to find a token listed on Binance with high expected volatility (and jumps) so that we can simulate multiple atomic swap events in a turbulent market environment. Initially, we looked for a token that appreciated a lot in price for the last 24 hours. We chose the BIFI[6]-USDT ticker to observe for a few hours as it exhibited 28.84% growth in the past 24 hours. The changes in the exchange rate are displayed in Figure 5. In line with our expectations, the rate experiences a severe correction in the first 5 hours, and then it recovers again back to the original rate in the next 10 hours.

During our calculations we assume that the BIFI-USDT ticker follows an MJD process in the observed time frame. We iterate through the exchange rates and measure the relative change between the natural logarithm of two adjacent data points (log-return). If the change is larger than a predefined threshold (ε) then we count the change as a stochastic jump in the exchange rate. With these assumptions we can calculate the necessary parameters ($\hat{\lambda}$ (jump intensity), $\hat{\sigma}_j$ (MJD std. deviation), $\hat{\mu}_j$ (MJD mean), $\hat{\sigma}$ (GBM std. deviation), $\hat{\mu}$ (GBM mean)) of the processes to simulate $SR(P^*)$ when one is trying to execute an atomic swap on the BIFI/USDT pair. The success rate is then calculated using (10). The parameters for the MJD model for the currrent simulation length (T$_{sim}$) are estimated based on [29] and we use the following values in the subsequent calculations:

Table I: Calculated MJD parameters from market data (hour units).

$\hat{\lambda}$ = 8.02	T$_{sim}$ = 20.69 h	$\hat{\sigma}_j$ = 0.0082
$\hat{\mu}_j$ = -0.000267	$\hat{\sigma}$ = 0.14	$\hat{\mu}$ = 0.0052

Then, in order to calculate *simulated* results we developed an open-source tool[7] using Python, which functions in the following way. The ticker data is tabulated such that there is a data point for every second. The script then chooses random points on the exchange curve and initiates an atomic swap process at each point by referencing the curve for price data at the strategic points in time. We then calculate the exact expected utility both for party A and party B using the ticker data.

At every point, the expected utility depends on the exchange rate (P^*) A and B agree on in the initial stage and this will define a price range tolerated by the users. We abort the swap once a party anticipates more utility from abandoning the deal (the observed price is out of the tolerated range) and continues otherwise. An attempt is calculated as failed if at any stage there is one party who chooses to abort the deal. The *simulated* success rate is calculated as the ratio between the number of successful swap attempts and the total number of attempts.

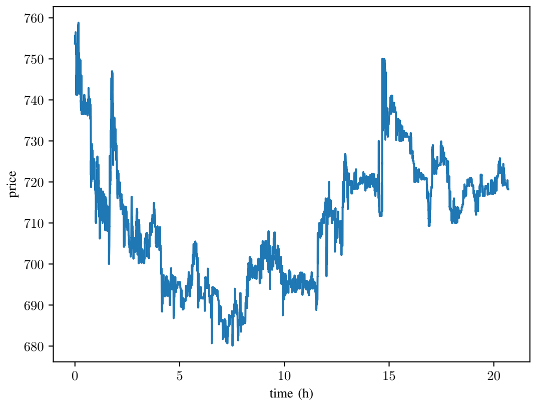

Figure 5: Real word trading data for the BIFI-USDT ticker from Binance between 2022-06-05 23:28 and 2022-06-06 20:09

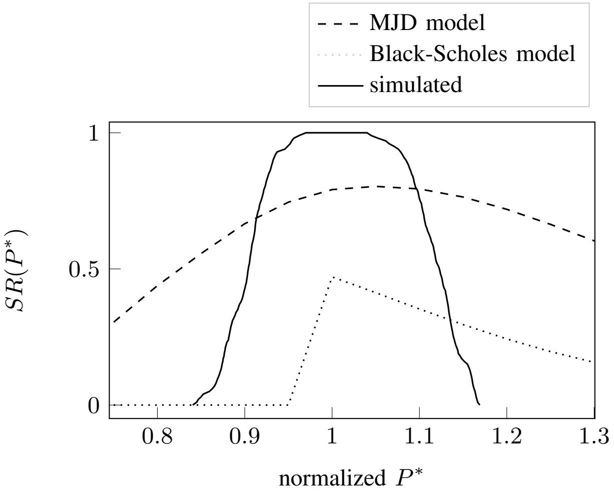

Figure 6: Simulated and estimated success rates calculated on the BIFI-USDT ticker dataset. The parameters for the stochastic estimation are taken from Table I and $\tau_a = 1$, $\tau_b = 1$, $\alpha_a = 0.2$ and $\alpha_b = 0.2$.

Results using the BS model, the MJD model and an actual simulation are presented on Figure 6. When $\varepsilon = 0.006$ we observe 8.06 jumps per hour and the measured σ is 0.14. These values are certainly attributable to a more hectic process than the ones that were analyzed on Figure 3. Based on our results we conclude that the BS model fails to properly describe this behavior, on the contrary the MJD model gives a much more realistic description of the success rate. Further improvements in both in the stochastic model and the simulation are required to present a more accurate interpretation of the process.

VII. Outlook and Conclusion

We understood that high price volatility and intensive jumps decrease the success rate of an atomic swap. Once the likelihood of a party anticipating significantly less utility due to

[5] https://github.com/binance/binance-spot-api-docs/blob/master/web-socket-streams.md

[6] https://beefy.finance/

[7] https://github.com/mlvl36667/mjd_atomic

an intensive downward price movement the incentive to stay in the deal disappears. This issue can be mitigated greatly if the parties exchange the ownership of an intermediary asset whose value does not change over time rather than the volatile assets. The success rate of exchanging the equivalent amount of stablecoins [30] between the two parties is clearly 1. In order to avoid the high volatility that is specific to crypto assets one could devise a protocol that would convert the assets to be exchanged into stablecoins on both chains and then perform an atomic swap between these stable assets with a probability equal to 1.

DAI[8] is a stablecoin project, whose currency still maintains its peg and users creating collateralized positions (CDP) can get hold of DAIs by depositing ETH to a smart contract. The amount of DAI issued in this process is determined by an algorithm, therefore the exchange is not fully trustless. Atomic swaps could be implemented by simply transferring the ownership of the CDP at the final stage and this would enable the receiving party to withdraw the requested amount of ETH from the contract. Unfortunately, the ERC-20 standard is specific to the Ethereum mainnet and there are not many blockchains with such abundant functionalities to implement stablecoins. Therefore our improvement proposal at this stage is merely theoretical.

In this work we examined the effect of unexpected jumps on the success rate of atomic swaps between two independent blockchains. We found that jumps in the exchange rate can significantly reduce the success rate of the atomic swaps and this can happen when markets are falling or appreciating rapidly. Additionally, we uncovered and interesting relationship between the intensity of jumps and the volatility of the price. Network delays, transaction confirmation times, and network partitioning attacks can render the atomic swaps vulnerable. The investigation of this issue shall also constitute a new direction for our future research activities.

References

[1] N. Satoshi, "Bitcoin: A peer-to-peer electronic cash system." 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] B. Cohen and K. Pietrzak, "The Chia network blockchain." 2019. [Online]. Available: https://www.chia.net/assets/ChiaGreenPaper.pdf

[3] M. Herlihy, B. Liskov, and L. Shrira, "Cross-chain deals and adversarial commerce," *Proc. VLDB Endow.*, vol. 13, no. 2, pp. 100–113, oct 2019. [Online]. Available: https://doi.org/10.14778/3364324.3364326

[4] F. Black and M. Scholes, "The pricing of options and corporate liabilities," *Journal of Political Economy*, vol. 81, no. 3, pp. 637–654, 1973.

[5] J. Xu, D. Ackerer, and A. Dubovitskaya, "A game-theoretic analysis of cross-chain atomic swaps with htlcs," in *International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2021, pp. 584–594.

[6] R. C. Merton, "Option pricing when underlying stock returns are discontinuous," *Journal of Financial Economics*, vol. 3, no. 1, pp. 125–144, 1976.

[7] M. Borkowski, D. McDonald, C. Ritzer, and S. Schulte, "Towards atomic cross-chain token transfers: State of the art and open questions within tast," *Distributed Systems Group TU Wien (Technische Universit at Wien), Report*, 08 2018.

[8] S. Johnson, P. Robinson, and J. Brainard, "Sidechains and interoperability," *arXiv preprint arXiv:1903.04077*, 03 2019.

[9] J. Xu, K. Paruch, S. Cousaert, and Y. Feng, "SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols," arXiv.org, Papers 2103.12732, Mar. 2021. [Online]. Available: https://ideas.repec.org/p/arx/papers/2103.12732.html

[10] I. Tsabary, M. Yechieli, A. Manuskin, and I. Eyal, "Mad-htlc: Because htlc is crazy-cheap to attack," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 1230–1248.

[11] P. Robinson, R. Ramesh, and S. Johnson, "Atomic crosschain transactions for ethereum private sidechains," *Blockchain: Research and Applications*, vol. 3, no. 1, p. 100030, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2096720921000257

[12] A. Dubovitskaya, D. Ackerer, and J. Xu, "A game-theoretic analysis of cross-ledger swaps with packetized payments," in *Int. Workshops Financial Cryptography and Data Security (FC)*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2021, pp. 177–187.

[13] J. Kirsten and H. Davarpanah, "Anonymous atomic swaps using homomorphic hashing," *Available at SSRN 3235955*, 08 2018. [Online]. Available: http://dx.doi.org/10.2139/ssrn.3235955

[14] R. Meyden, "On the specification and verification of atomic swap smart contracts (extended abstract)," *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 05 2019.

[15] M. Herlihy, "Atomic cross-chain swaps," in *ACM symposium on principles of distributed computing (PODC)*, 07 2018, pp. 245–254.

[16] M. Belotti, S. Moretti, M. Potop-Butucaru, and S. Secci, "Game theoretical analysis of cross-chain swaps," in *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, 11 2020, pp. 485–495.

[17] Y. Xue and M. Herlihy, "Hedging against sore loser attacks in cross-chain transactions," in *ACM Symposium on Principles of Distributed Computing (PODC)*. New York, NY, USA: Association for Computing Machinery, 2021, pp. 155–164. [Online]. Available: https://doi.org/10.1145/3465084.3467904

[18] R. Han, H. Lin, and J. Yu, "On the optionality and fairness of atomic swaps," in *ACM Conference on Advances in Financial Technologies (AFT)*. New York, NY, USA: Association for Computing Machinery, 2019, pp. 62–75. [Online]. Available: https://doi.org/10.1145/3318041.3355460

[19] J. C. Cox, S. A. Ross, and M. Rubinstein, "Option pricing: A simplified approach," *Journal of Financial Economics*, vol. 7, no. 3, pp. 229–263, 1979. [Online]. Available: https://www.sciencedirect.com/science/article/pii/0304405X79900151

[20] S. Tang and S. S. M. Chow, "Systematic market control of cryptocurrency inflations," in *ACM Workshop on Blockchains, Cryptocurrencies, and Contracts (BCC)*. New York, NY, USA: Association for Computing Machinery, 2018, pp. 61–63. [Online]. Available: https://doi.org/10.1145/3205230.3205240

[21] J. A. Liu, "Atomic swaptions: Cryptocurrency derivatives," *ArXiv*, vol. abs/1807.08644, 2018.

[22] J. Rueegger and G. S. Machado, "Rational exchange: Incentives in atomic cross chain swaps," in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2020, pp. 1–3.

[23] O. Goldreich, S. Micali, and A. Wigderson, "How to prove all NP statements in zero-knowledge and a methodology of cryptographic protocol design (extended abstract)," in *Advances in Cryptology — CRYPTO' 86*, A. M. Odlyzko, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1987, pp. 171–185.

[24] R. L. Rivest and M. L. Dertouzos, "On data banks and privacy homomorphisms," 1978.

[25] C.-P. Schnorr, "Efficient identification and signatures for smart cards," in *CRYPTO*, 1989.

[26] V. Zakhary, D. Agrawal, and A. Abbadi, "Atomic commitment across blockchains," *arXiv preprint arXiv:1905.02847*, 05 2019.

[27] J. Gugger, "Bitcoin-monero cross-chain atomic swap," *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 1126, 2020.

[28] L. Fournier, "One-time verifiably encrypted signatures a.k.a. adaptor signatures," 2020.

[29] F. Tang, "Merton jump-diffusion modeling of stock price data," 09 2018. [Online]. Available: http://lnu.diva-portal.org/smash/get/diva2:1257256/FULLTEXT01.pdf

[30] A. Moin, E. Sirer, and K. Sekniqi, "A classification framework for stablecoin designs," *arXiv preprint arXiv:1910.10098*, 09 2019.

[8] https://makerdao.com/en/