Blitzkrieg: Off-Chain Payment Routing

Guy Fawkes
guyfawkesfp@protonmail.com
https://discord.gg/z2bZEq2

Abstract. Off-chain transactions would allow Bitcoin payments to be settled instantly, privately, and with low fees. Payment channels provide part of the solution, but the main benefits are lost if routing payments require immobile centralized hubs. We propose a solution to the routing problem using probabilistic payments. The network routes payments from sender to recipient through provable games of chance. Games of chance yield an expected value equivalent to payment, while reducing the frequency of on-chain settlement. Finders distribute staked funds. Users join pools to hedge volatility. Through this process a near-complete graph is formed, negating positional advantage among pools.

1. Introduction

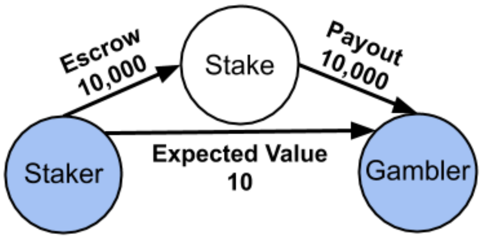
Scaling Bitcoin off-chain has come to rely on routing multi-hop payments through a network of bi-directional payment channels. A bi-directional payment channel is sufficient for an on-going relationship between two parties, but multi-hop payments still suffer from the inherent weakness of finding a liquid path across the network. The challenge is made exponentially more difficult when routing large payments. As a result, nodes are incentivized to make connections at central locations to increase the probability of finding a route. This leads to a network effect among well connected nodes to the detriment of less liquid smaller nodes. While smaller competing nodes can create alternative connections away from central hubs, they are fundamentally disadvantaged due to additional hops and limited liquidity. All these incentives bring censorship resistance of the network into question.

What is needed is a way for sender and recipient to facilitate an off-chain payment without first establishing an on-chain relationship. Off-chain transactions that do not require a pre-existing payment channel would alleviate the burden of finding a liquid route across the network. The main benefit would be equal network position among nodes, regardless of scale. In this paper, we propose a solution to the routing problem using probabilistic payments to indirectly connect all senders to all recipients.

2. Probabilistic Payments

To simplify off-chain Bitcoin payments, an already established property of Bitcoin mining can be used. Today, Bitcoin miners engage in trillions of transactions per second. These transactions are what many call hashes. While miners are not paid on a per hash basis, the expected value of each hash can be viewed the same as payment. In the long run, actual mining rewards collected converge toward expected value per hash.

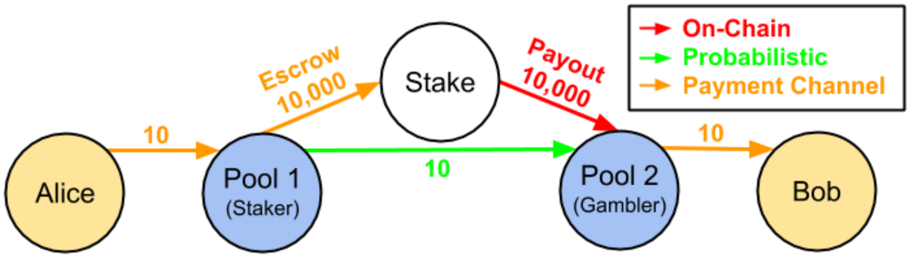
The same settlement property can be applied to off-chain Bitcoin payments. Two counterparties seeking to make an off-chain transaction agree to a game of chance. Let's say a staker and a gambler agree to a payout of 10,000 units, with odds of 1,000:1. The staker stakes 10,000 units. If the gambler wins the game, it wins 10,000 units. If the gambler loses the game, it wins nothing. The expected value of each game is 10 units from the staker to the gambler, while on-chain settlement will only occur on average every 1,000 payments.



The obvious benefit is both parties can execute a payment with significantly reduced on-chain settlement. The not so obvious benefit is the staker and gambler can execute off-chain payment without pre-establishing an on-chain payment channel, in doing so, indirectly connecting all nodes to all nodes. While the game of chance simplifies routing, the variance associated with payment would be impractical for most use cases. The user needs a way to be protected from payout variance.

3. Variance and Payment Channels

Our solution begins with pooling payments. Similar to how miners join pools to reduce variance in payouts, users can join pools to reduce variance in probabilistic payments. The staker and gambler then assume the role of pool operators, and open bi-directional payment channels with their pool members. Let's say Alice wants to pay Bob 10 units. Alice is a member of Pool 1; Bob is a member of Pool 2. Both Alice and Bob have bi-directional payment channels with their pools. Alice sends 10 units to Pool 1 via payment channel. Pool 2 sends 10 units to Bob via payment channel. Pool 1 and Pool 2 engage in a probabilistic payment, completing the route of 10 units from Alice to Bob.



Alice and Bob are protected from payout variance, while achieving instant, off-chain, settlement. Additionally, Pool 1 and Pool 2 can easily connect regardless of network position. The remaining challenge is how does the gambler trust the staker to offer a fair game of chance, and pay out in the event of a win.

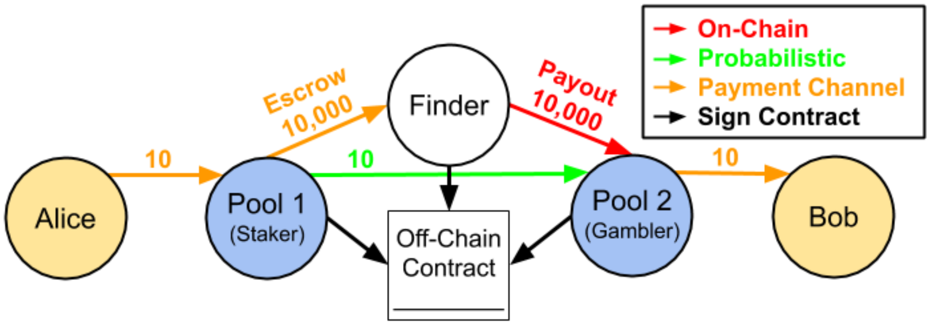
4. Provable Game of Chance

To create a provably fair game of chance, the staker and gambler jointly create a seed used for determining the winner. The staker generates half of the seed and hashes it. The gambler generates half of the seed and hashes it. Before the game is played, the staker and gambler exchange hashes and agree to how the two seeds will be interpreted in determining the winner. After the game of chance is played, both parties reveal their respective half of the seed to prove the game was fair. The challenge then becomes, how are seeds exchanged to determine the winner, and how are staked funds distributed.

5. Staked Funds

The lowest trust option for determining a winner and distributing staked funds would likely involve a smart contract. Inter-pool payments could be settled on a smart contracting platform, while payment channels could be settled on Bitcoin. In our estimation, a smart contract setup would only require the gambler to trust that a colluding staker and finder do not double-spend a winning contract. Otherwise, the finder would not be able to run off with the stake.

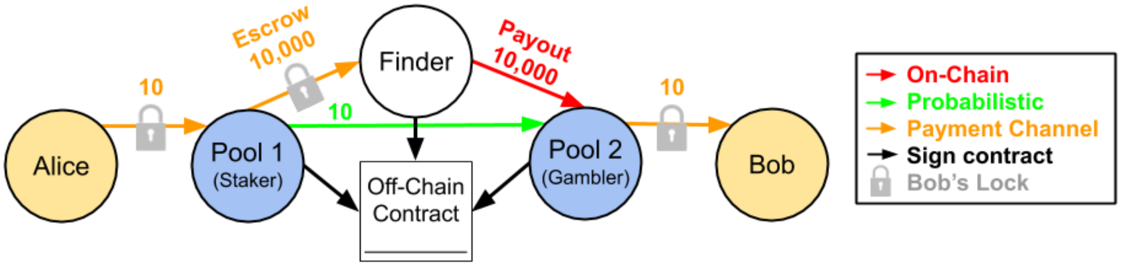
To illustrate how staked funds can be distributed using only Bitcoin, we consider a simpler approach of a mutually trusted finder escrowing funds. Pool 1 chooses a finder, and makes a connection via payment channel. The payment channel allows Pool 1 to rapidly load and unload its stake with the finder to reduce risk. Pool 2 must trust the pre-selected finder of Pool 1. If the gambler trusts the finder, then all three parties agree to an off-chain contract.



While the off-chain contract is non-binding, it enables either pool to publicly protest the decision against the reputation of the finder. This of course brings the challenge of the “He said she said” problem.

6. Payment Sequence & Deterministic Disputes

The payment sequence is designed in such a way to accurately and deterministically prove the proper outcome of the game of chance. While the finder is still trusted to distribute staked funds, the staker and gambler are able to provably document a cheating finder to the greater network. The staker, gambler, or finder can start the dispute process by submitting on-chain, the off-chain contract. This provides proper notice to the relevant counterparties, and proves to the greater network that all parties to the contract are given proper notice of dispute. Disputes are evaluated on a guilty until proven innocent basis. After the on-chain claim, the dispute process is resolved deterministically. Finders and pools are required to submit relevant information as prescribed by the off-chain contract, otherwise it is assumed they are cheating. The sequence is as follows:



Off-Chain Contract Steps

1. Bob submits hash lock.
2. Pools 1 & 2 submit respective game seed hashes.
3. Pools 1 & 2 submit respective payout addresses.
4. Pools 1 & 2 agree to odds/interpretation.
5. Pools 1 & 2 agree to deadline for valid on-chain disputes and the blockchain disputes will be settled on.
6. Pool 2 signs contract.
8. If Alice does not load, then Pool 1 terminates contract. If Alice loads, then Pool 1 signs contract.
10. If Pool 1 does not load, then Finder terminates contract. If Pool 1 loads, then Finder signs contract.
14. Gambler sends its game seed to Finder.
16. Staker sends its game seed to Finder.
19. Finder discloses Bob's seed to Alice, and Alice's seed to Bob to prove game was fair.

Payment Steps

7. Alice loads hash lock contract unlockable by Bob's password.
9. Pool 1 loads hash lock contract unlockable by Bob's password on channel with Finder.
11. Finder tells Pool 2 safe to load, then Pool 2 loads hash lock unlockable by Bob's password.
12. Bob claims funds, revealing password to Gambler.
13. Gambler sends Bob's password to Finder, so Finder can receive staked funds.
15. Finder claims funds, revealing password to Staker.
17. Staker claims funds from Alice.
18. If Gambler loses, Finder returns escrow to Staker in payment channel. If Gambler wins, Finder sends 10,000 on-chain to Gambler.

20. Dispute Process

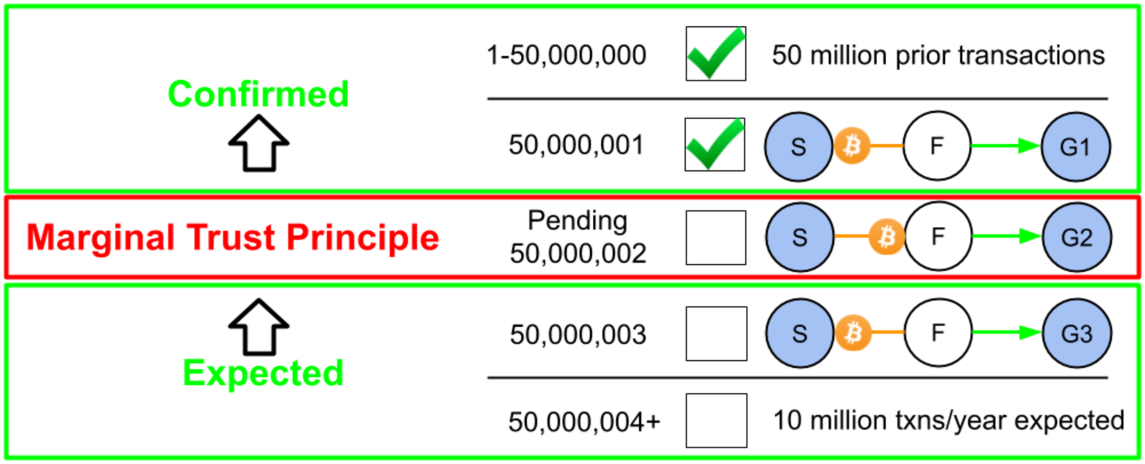
0. Disputing party makes valid claim if published off-chain contract is within deadline and on relevant blockchain (Step 5). If either condition is not satisfied, then contested parties need not respond.
1. Gambler reveals Bob's password by first deadline.
-If not, Gambler is assumed to have "Locked Funds."
2. Both Staker and Gambler reveal game seeds by second deadline.
-If not, withholding party loses game of chance by default.
3. If Gambler wins game of chance, Finder must submit payment to relevant address (Step 3) by third deadline.
-If not, it is assumed Finder has cheated.
3. If Staker wins game of chance, and is claiming Finder broke contract, Staker closes payment channel. Funds must be in relevant address (Step 3) by third deadline.
-If not, it is assumed Finder has cheated.

There is a concern with respect to denial of service involving Bob or the gambler locking the staker's funds in escrow until the time lock expires. To mitigate this scenario, the pools can optionally agree to a "Locking" payout in the off-chain contract, for which the gambler would be expected to pay in the event it is found to be "Locking funds."

Another concern is the on-chain dispute process would take considerable time and incur large on-chain fees. To mitigate this problem, contract disputes can be made in somewhat real time on a separate public "Federated blockchain," while all payments remain on Bitcoin. Contract disputes are likely not impacted by the security assumptions of a "Federated blockchain" model.

7. Marginal Trust Principle

The obvious questions remains, what is the risk exposure to the finder? Alice and Bob need not trust the finder. The gambler and staker have limited trust in the finder, due to the marginal trust principle. The finder is only capable of stealing funds that are actively in transit. Funds waiting in line and funds that have already been routed are not exposed. Because the gambler and staker can provably document a cheating finder, the finder gets one exit scam before it is presumably blocked by the greater network. The goodwill value of a reputable finder will likely exceed the value of an exit scam by many multiples.



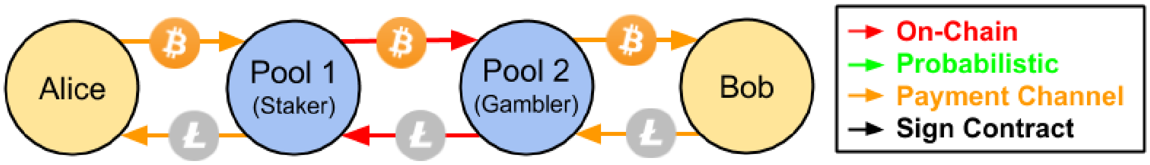
Many will argue the finder is a trusted entity and therefore an inherent flaw to the payment network. The important distinction to be made is that while the finder is a trusted entity, it does not create a central point of failure to the greater network. Imagine the network of finders as a dam safely redirecting water downstream. Many attackers will attempt to poke holes in the dam stealing water and attempting to collapse the greater structure. While holes will be made, and some water will be lost, the marginal trust principle immediately seals up any cracks. Pools price in lost water, and users are not exposed to variance. The dam still functions in a sustainable, cost-efficient way.

8. Privacy

Without privacy, the man with the biggest gun essentially controls the network. This proposal affords a high degree of privacy in payment. Most payments settle off-chain. The few payments that do settle on-chain are from pool-to-pool, or when the user closes out its payment channel. The primary concern with regard to protocol-level privacy is the user's exposure to the gateway pool. The gateway pool is the pool the user directly connects to. This pool has nearly all the transactional data of the user. Additionally, some metadata regarding amount and time is leaked to the related finder and counterparty pool. It should be noted there are layers which can be added to obfuscate user-pool connections as well as pool-pool connections.

9. Decentralized Spot Exchange

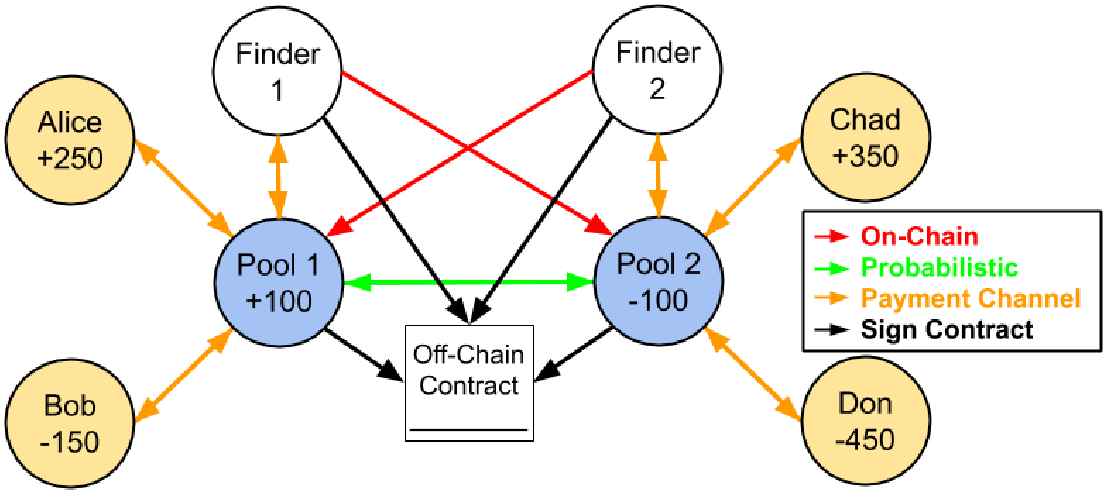
This proposal can similarly reduce the routing problem associated with decentralized exchange. Imagine if each pool acts as a node within a greater decentralized exchange. While the same general routing process occurs, probabilistic payments are not feasible for inter-pool transfers. As settlement for probabilistic payments are infrequent, it would give pools significant exchange rate exposure to cryptoassets. Instead, inter-pool transfers utilize on-chain atomic swaps. Users get simple instant settlement, while pools facilitate difficult on-chain delivery.



The problem is each pool would need sufficient liquidity of many cryptoassets for all of its users. This would presumably centralize pools and bring censorship resistance of the exchange network into question. To reduce the inventory burden, pools can instantly sell derivatives contracts to the user (against the user-pool payment channel), while the pool secures the on-chain underlying from another pool. After securing the on-chain asset, the pool can deliver the underlying to the user and close out the derivative contract.

10. Decentralized Stablecoin & Derivatives

Probabilistic payments create the basis for a Bitcoin-backed stablecoin through the use of derivatives. A stablecoin running on Blitzkrieg requires little collateral exposure due to rapid settlement enabled by payment channels and probabilistic payments. Users and pools can reliably collateralize positions while actively staking as little as 1% of notional value. For example, Alice is long 250, Bob is short 150, for a net position of 100 long for Pool 1. Pool 2 has a net position of 100 short. Pool 1 and Pool 2 agree to an off-chain contract detailing terms and cancelling out their respective exposure.

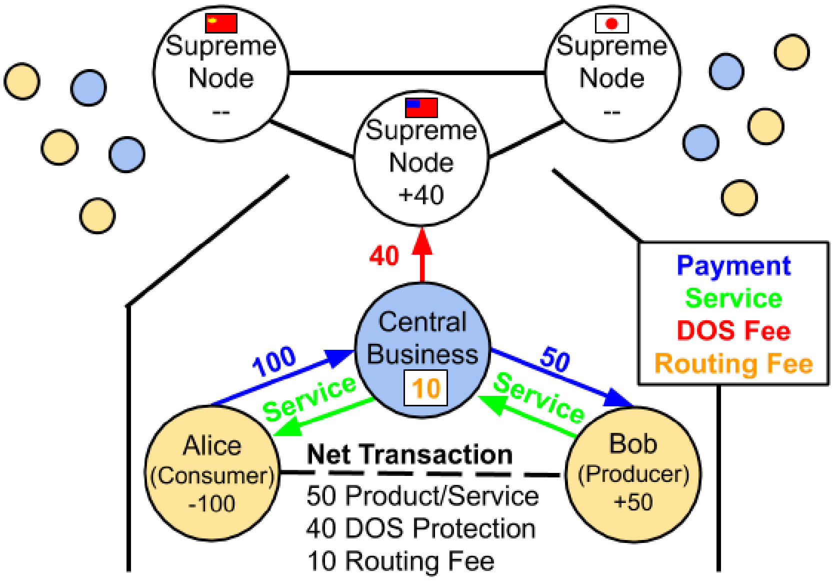


In both user-pool and pool-pool connections, very little collateral needs to be actively staked. For example, Alice can perpetually update the balance of her bi-directional payment channel with Pool 1 to have exactly 2% collateral staked against her open position at all times. A similar property applies to inter-pool contracts. Pool 1 and Pool 2 stake 1% of position size as collateral with their respective finders and agree to settle position imbalances through probabilistic payments every 0.25% deviation in collateral. If Pool 1 is unresponsive, or otherwise cannot rebalance the position, Pool 2 can reclaim relevant collateral from Finder 1, and quickly find an opposing counterparty in the open market. The same process can be applied to trade derivatives on any asset.

The strength of the derivatives network is derived from the ability for pools of all sizes to combine liquidity, while remaining segregated entites. A would be attacker would have to take down pool by pool, and finder by finder. The damage done would be limited to the small amount of collateral actively staked by users and pools. The attacker would have little ability to prevent new pools and new finders from joining the network in response to the attack.

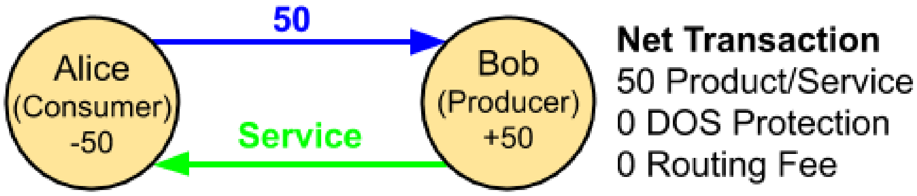
11. Limitation of Bitcoin and Blitzkrieg

Bitcoin enables secure one-way value transfer. Bitcoin is secure to the extent that Alice pays Bob. The fundamental limitation of Bitcoin is when it used in two-way value transfer. In other words, Alice can securely transfer Bitcoin to Bob, but Bob cannot securely transfer physical products and services to Alice. Thus, Bitcoin is only as secure as the products and services for which it can actually be exchanged for. Below is a purely hypothetical network of two-way value transfer.



Alice wants to purchase a service. Bob wants to provide a service. Alice and Bob both connect to a central business routing node that connects the two for trade. Alice pays the business node 100 units. The business node pays Bob 50 units. One might ask where the other 50 units goes. The business node keeps 10 units as a routing fee. The other 40 units are paid to the local supreme node for DOS protection. Without DOS protection, the central business node is unable to route products and services. The end result is Alice pays Bob 50 units, while incurring another 50 units in DOS and routing fees. Whether Alice pays Bob with Bitcoin, Blitzkrieg, Gold, or green toilet paper, all exchanges within this network will still be subject to the same DOS and routing fees. In other words, Bitcoin has little utility in legacy trade networks.

Bitcoin's utility comes from its ability to evade DOS and routing fees. Without a way to securely exchange physical products and services for Bitcoin, Bitcoin has little utility. Fortunately, there is a solution. The nimble user nodes outnumber the supreme node members 1000:1. The supreme nodes do not have the capacity to DOS attack the abundant number of user nodes. If the user nodes route products and services directly peer-to-peer, without going through a central business node, they can evade DOS fees and routing fees.



Peer-to-peer trade enables secure transfer of physical products and services. Bitcoin enables secure transfer of electronic cash. If paired together, Alice can save up to 50% on trade by eliminating DOS fees and routing fees. A proposal for secure peer-to-peer trade is detailed in the Freedom Network whitepaper:

https://drive.google.com/file/d/1SnRdVeGoPkkdk2lXtdjDfy7c0z1ZlmRE/view?usp=sharing

12. Conclusion

We have proposed a system for off-chain Bitcoin payments without the user relying on trust. We started with probabilistic payments, which connect all senders to all recipients, but is incomplete without a way to reduce payout variance and distribute staked funds. To solve this, we proposed users join pools to obviate payout variance, while staked funds are distributed by trusted finders accountable to deterministic public disputes. Increased connectivity between pools enables decentralized exchange, and a low trust Bitcoin-backed stablecoin. Users enjoy instant, private settlement, while placing no trust in finders or pools. Finders are affirmed by pools, and pools are affirmed by users. Any needed rules and incentives can be enforced with this consensus mechanism.