HashRaffle: A Self-Sustaining Platform to Fund Growth of the Peer-to-Peer Cash Ecosystem by Utilizing Provably-Fair Bitcoin Cash Raffles and the Simple Ledger Protocol

shraffle@hashraffle.cash
https://hashraffle.cash

Abstract: We propose a free-market mechanism, based on provably-fair raffles, to fund development of Bitcoin Cash (BCH) and use cases built on top of it which will further BCH's maturation into peer-to-peer (P2P) cash for the world. Greed is a powerful force which provides seemingly unlimited demand for potentially profitable games of chance. A raffle based on BCH can harness that greed and turn it into a renewable source of funds to support developers, projects, and startups that contribute to the P2P cash ecosystem; and to create bounties for desired features and initiatives. A raffle whose winner is found by hashing strings made up of transaction IDs, nonces, and the hash of a specific block in the future; and identifying the lowest alphanumeric value out of the results is provably fair. The raffle prize is split between the raffle winner and a specific beneficiary identified before the contest. Raffle entrants are rewarded with the Simple Ledger Protocol (SLP) token "Raffle Cash" (RAFL) that they can send to developers, organizations, or entrepreneurs who they think ought to be a beneficiary of a raffle. Those with RAFL tokens can trade a specified amount of them for a spot as a raffle beneficiary with HashRaffle. HashRaffle necessarily verifies the legitimacy of potential beneficiaries based on reputation and track record as allies and builders of P2P cash or related applications.

1. P2P Cash, Decentralization, and Greed

We believe that Bitcoin Cash is meant to be P2P cash for the entire world and this proposal is a reflection of that, attempting to spark further development towards that goal. P2P cash ought to be accessible to as many people as possible, with the least amount of friction. This necessitates low-cost on-chain capacity for everyday spending for anyone who desires to transact. Many developments and innovations are required, not only to make on-chain capacity for the world a reality, but to enable all the features and components that the market demands for borderless, electronic P2P cash. HashRaffle aims to encourage and incentivize people to contribute to these required developments for Bitcoin Cash.

P2P cash cannot be centralized. That is to say that any currency that is centralized cannot become true P2P cash as it will inevitably become controlled and regulated by gatekeepers. Fiat currencies and associated services have become so inflated, overly regulated, and inaccessible precisely because of central authorities and their desire for control. We have even seen promising cryptocurrencies and their communities fall victim to the problem of centralized control. Centralization represents an attack vector, easily exploited by those who want to prevent true P2P cash from becoming a reality. If Bitcoin Cash is to become P2P cash for the world, it has to pursue that goal using means as worthy as the lofty ideals of the end in mind. So far Bitcoin Cash has managed to follow this development path and HashRaffle is dedicated to continuing that trend.

HashRaffle uses permissionless systems to provide a funding platform for the development of Bitcoin Cash, its use cases, and any efforts to increase adoption and utility. HashRaffle aims to be a new approach that complements the other permissionless funding initiatives in the community, contributing to the overall decentralized structure that directs funds to where they are needed. HashRaffle's approach specifically leverages greed, which is a powerful motivator not to be dismissed out-of-hand. Even those that look down upon games of chance should recognize that it can be a purely voluntary act. Those who play games like raffles ought to play games that are provably fair and as inexpensive and frictionless as possible. HashRaffle provides that. If HashRaffle can attract people who would play games of chance, regardless of who is running them and why, the actions of those people can be harnessed to benefit all of society by funding the growth of P2P cash.

2. Raffle

Each raffle on HashRaffle results in one winner and also benefits one specific entity in the BCH ecosystem identified beforehand. HashRaffle runs one raffle at a time to prevent different initiatives from competing against each other for funding and to create a larger, more attractive prize for raffle players. Each raffle uses a single BCH address to accumulate the funds for the duration of the round. One enters the raffle by purchasing one or more tickets, with each ticket representing one chance to win the raffle out of the total number of tickets sold during the round. The only action necessary to enter the raffle is to send a BCH amount to the raffle address equal to the ticket price multiplied by the number of tickets desired. For example, if a raffle ticket costs 0.1 mBCH and one wants to purchase 100 tickets, one would send 10 mBCH to the raffle address in a single transaction. We expect the price of each raffle ticket to be somewhere between the equivalent of USD $0.01 and $0.10 to maximize accessibility and allow anyone in the world to play the raffle. The price of a ticket in terms of BCH may change over time as the value of BCH fluctuates relative to fiat currency.

Each raffle ticket is an alphanumeric value that consists of the transaction ID (TXID) of the transaction used to purchase the ticket concatenated with a nonce that ranges from 0 to the number of tickets purchased in that transaction less 1. For example, if one purchases one ticket, the nonce concatenated with the TXID is 0. If one purchases ten tickets, the nonce concatenated with the TXID on each of the ten tickets is each number from 0 to 9.

At the start of a raffle, a block in the future is publicly identified that signals the end of the round. That block can be defined by a specific block height, by the nth block before or after a specific date and time, or by some other manner. Only raffle tickets purchased with transactions confirmed in or before the specified ending block are considered valid for the raffle contest. After the specified block has been added to the blockchain (with some number of confirmations to be sure it is not orphaned) each raffle ticket (a concatenation of the TXID and a nonce) will be concatenated with the hash of the block that ends the raffle. The entire concatenated string of each ticket with the block hash is then hashed using the SHA-256 function. After each ticket has undergone this process, all the ticket hashes are sorted alphanumerically. The ticket hash with the lowest alphanumeric value is the winner of the raffle.

3. Raffle Winnings

When a raffle has ended and the winner has been decided, the BCH in the raffle address can be disbursed. At least 2/3 of the total funds in the address are split equally between the raffle winner and the raffle beneficiary. HashRaffle sends the prize money to the raffle winner by sending their portion to the address that provided the input 0 in the transaction used to purchase the winning ticket. HashRaffle sends the funding portion of the raffle to the beneficiary using an address the beneficiary chooses.

No more than 1/3 of the total funds in the raffle address are used to seed the next raffle and for HashRaffle's administration fee. Having a portion of each raffle seed the next keeps each round attractive to prospective raffle ticket buyers at the outset. No more than 5% of the total funds in the raffle address are used for HashRaffle's administration fee. The administration fee pays for the costs associated with hosting and promoting the raffle. We expect the ratio of the prize and beneficiary money to the money used for seeding and administration fees to increase over time as HashRaffle gains more players and the raffles become more self-sustaining.

4. RaffleCash SLP token

The RaffleCash (RAFL) SLP token forms an integral part of the HashRaffle strategy. The Token ID is 3b7a24d664058feb49f4d57c40a7563e3257891495aefd1fd1015c90a9d9f988. For every 1 mBCH (0.001 BCH) spent on raffle tickets, a raffle player receives 1 RAFL in return. Players can receive fractions of RAFL for BCH spent on tickets. There may be incentives in place that require players to buy a certain number of tickets to qualify to receive RAFL. The RAFL is sent to the address that provides the input 0 of the transaction used to purchase tickets, converted to its corresponding SLP address.

We do not expect the exchange rate of 1 RAFL/1 mBCH to change, even if the raffle ticket prices change. Fixing the RAFL/BCH exchange rate rather than letting it track raffle ticket prices (which we expect to reduce as BCH's value rises) should prevent RAFL emission from experiencing any sudden massive increases, except in the case of a sudden rise in HashRaffle's popularity or a sudden crash in BCH's value. This will prevent holders of RAFL from having their "voting power" suddenly diluted if HashRaffle lowers raffle ticket prices.

Holders of RAFL may send their tokens to individuals or organizations that hope to secure a spot as a raffle beneficiary or keep their tokens if they themselves hope to become a raffle beneficiary. We expect BCH developers and teams to solicit contributions of RAFL from the pool of HashRaffle players. It is even possible that a market for RAFL develops independent of HashRaffle as those who want to secure funding on HashRaffle try to obtain the token.

The existence and implementation of the RAFL SLP token creates a layer of community ownership and direction over what to fund in the P2P Cash ecosystem. In effect, taking part in raffles on HashRaffle grants the players the ability to vote on the projects they would like to see thrive, but in a purely voluntary and permissionless fashion. We do not expect all raffle players to care about or use their RAFL tokens and they do not have to. HashRaffle is set up so that raffle players can just be raffle players without having any involvement in the greater P2P cash community. But a portion of the BCH they spend on raffles goes towards development, new features, and P2P cash applications. The RAFL token empowers the raffle players that are involved in the P2P cash community to direct those funds and make a difference.

5. Raffle Beneficiaries

Available spots for raffle beneficiaries on HashRaffle are advertised ahead of time along with their price (in RAFL). However, raffle beneficiary spots cannot simply go to any person or organization with the required amount of RAFL, as that would open up an attack vector to those hostile to P2P cash. Therefore, an application process for potential beneficiaries must be in place.

To be considered for a beneficiary spot, a prospective beneficiary must have already contributed to P2P cash in some useful, verifiable way. Those considering purchasing a spot as a raffle beneficiary should expect to disclose to HashRaffle their contributions to P2P cash and have those contributions verified. Previous raffle beneficiaries desiring further funding should expect to answer questions about, and provide evidence for, how the funds from prior raffles were used. Accepting an individual or group as a raffle beneficiary is at the sole discretion of HashRaffle, but potential beneficiaries who operate according to the principles of P2P cash outlined in the first section of this paper should have no problem being accepted if all the necessary conditions are met.

If an individual or organization is found to be a suitable raffle beneficiary, an SLP address will be provided to them to officially purchase an available spot through a RAFL token transaction. RAFL used to purchase a spot as a raffle beneficiary will be burned. Raffle beneficiaries are urged to provide statements and other information about themselves and what they plan to use funds for that HashRaffle can use to market the raffle to potential players.

It is possible that some available beneficiary spots remain unclaimed. This is particularly possible when HashRaffle is starting out. In such an event, HashRaffle reserves the right to give an unclaimed beneficiary spot to any individual or group developing or otherwise contributing to

P2P cash for the world. With that being said, HashRaffle itself will never be a beneficiary for its own raffle as that would create a clear conflict of interest.

6. Bounties

HashRaffle can accommodate the desire to fund initiatives and features for P2P cash that do not yet exist, even if no one is currently planning to work on them. The community can make suggestions for such things that they would like to see developers and entrepreneurs rewarded for through a bounty. A bounty web page can display all potential bounties approved by HashRaffle, their associated SLP addresses that people can donate RAFL to, and the precise conditions required to collect the bounty once it exists.

When a potential bounty's SLP address has received RAFL equal to the amount of RAFL required to be a beneficiary, the next available raffle can be used to fund that bounty. Alternatively, if a beneficiary for an upcoming raffle has not been selected, the beneficiary spot may go to the bounty with the highest balance of RAFL in its SLP address. After a bounty has been funded by one or more raffles, the conditions that need to be met in order to collect the bounty are made available. Any individual or organization that believes they have fulfilled the conditions to collect a bounty can contact HashRaffle. If the conditions have been met, the bounty is paid out to an address the bounty collector chooses.

7. Trust

Raffle players and those who wish to fund the P2P cash ecosystem surely value a very high level of trust when purchasing raffle tickets and funding raffle beneficiaries. Steps can be taken to establish that trust. In cases where HashRaffle does not unilaterally choose a beneficiary, HashRaffle and the beneficiary may create a multi-signature wallet to generate the address used for that particular raffle. Additionally, HashRaffle is incentivized to only accept reputable individuals and organizations that have goodwill in the community as raffle beneficiaries.

It is important that the entire raffle process be transparent and auditable by anyone. Using a single BCH address for each raffle ensures a relatively simple process for auditing the raffles and ensuring that the raffle rules are followed. Anyone that is able and willing to view the BCH blockchain can repeat the process for finding a raffle winner and verify that the correct winner is chosen. For convenience, information on each raffle is retained and made available for any interested parties.

It is also important that raffle players and those in the P2P cash community trust that the RAFL token distribution is fair and that there is no abuse happening that influences who receives a spot as a raffle beneficiary. The Simple Ledger Protocol (SLP) makes such things simple to verify. Anyone willing to inspect SLP transactions can find that newly-minted RAFL tokens are only sent to either: 1) SLP addresses corresponding to BCH addresses used as the input 0 in transactions for purchasing raffle tickets or 2) SLP addresses of those who have provided funds to seed raffles. In either case, the tokens are distributed at a rate of 1 RAFL per 1 mBCH spent on a raffle or on seeding a raffle (provided any applicable minimums are reached). It is important to note here that HashRaffle reserves the right to use its own funds to seed raffles and receive RAFL in return (which does not apply to carryover seeding from a prior raffle). It is also verifiable that RAFL tokens sent to HashRaffle to purchase a beneficiary spot are not reused or held long-term, but are burned. Information on the purchases of beneficiary spots is retained and made available for any interested parties.

8. Conclusion

We have proposed that provably-fair raffles can form a self-sustaining mechanism for funding progress and development in the Bitcoin Cash ecosystem. A feedback loop of properly-aligned incentives should keep funding for P2P cash viable into the foreseeable future without overly relying on BCH "whales" who are perhaps too often called upon to fund the ecosystem's most important initiatives. HashRaffle is incentivized to continually run highly-accessible, provably-fair raffles that benefit developments the BCH community finds credible, crucial, and exciting; and that prospective raffle players outside the BCH community find attractive. Individuals and organizations in the BCH community that desire funding and support have the incentive to solicit RAFL donations, thus steering their supporters to HashRaffle; and the incentive to market the raffles that fund either themselves or others that contribute to their efforts. Long-term holders of BCH and other BCH stakeholders are incentivized to see HashRaffle flourish so that new funds can enter the ecosystem through a fresh approach. Simple greed and a low-cost entry attracts and motivates raffle players to purchase as many raffle tickets as necessary to reach acceptable odds of winning the raffle prize money. Raffle players who value P2P cash have the incentive to purchase tickets to fund their favored projects, persuade others to do the same, and send their RAFL tokens to worthy causes that increase the value of the cryptocurrency they have chosen to use and have a chance to win.

Appendix: A Simplified Raffle Example

A simplified example of a raffle demonstrates how the contests function. A raffle was simulated on the address qzcylh2g7fuxn2gkc2cp3eddc4nzegz00qp6sdqt4s with a ticket price of 0.1 mBCH and the contest ending on the last block before 01-01-2021 00:00 (UTC).

The first transaction sent to the contest address,

ab1e563a572f9274c1ce4f1c22d3ae365258e774e52fb9da25b26086b2466b04

was for seeding the round and is ignored for the purposes of finding the raffle winner. The final transaction sent to the contest address during the raffle,

002fc5117ca186b2dccc119b0898ad28a2352af85ecce9dbd0f26769d8cec2fb was for an amount less than the price of a single ticket and is also ignored. There are three remaining transactions that purchased tickets. Their TXIDs are:

```
9d055e4a49bea54f2733758377a65169f4f8b50a4984272daa927b10027b20df
d2b4f0aeb943df16f538a714b10457938cc38d3906b1bed8e5cb953bfd13cde2
3ff9ba6f8008cacc89d36867e769533484a53b59fd74ecafeb2ead7be54dbc05
```

TXID 9d05...20df was for 0.1 mBCH which earns that entrant 1 ticket. That single ticket consists of the TXID concatenated with 0. Thus, the single ticket is:

```
9d055e4a49bea54f2733758377a65169f4f8b50a4984272daa927b10027b20df0
```

TXID d2b4...cde2 was for 0.2 mBCH which earns that entrant 2 tickets. Those tickets consist of the TXID concatenated with 0 and 1. Thus, the 2 tickets are:

```
d2b4f0aeb943df16f538a714b10457938cc38d3906b1bed8e5cb953bfd13cde20
d2b4f0aeb943df16f538a714b10457938cc38d3906b1bed8e5cb953bfd13cde21
```

TXID 3ff9...bc05 was for 0.5 mBCH which earns that entrant 5 tickets. Those tickets consist of the TXID concatenated with 0, 1, 2, 3, and 4. Thus, the 5 tickets are:

```
3ff9ba6f8008cacc89d36867e769533484a53b59fd74ecafeb2ead7be54dbc050
3ff9ba6f8008cacc89d36867e769533484a53b59fd74ecafeb2ead7be54dbc051
3ff9ba6f8008cacc89d36867e769533484a53b59fd74ecafeb2ead7be54dbc052
3ff9ba6f8008cacc89d36867e769533484a53b59fd74ecafeb2ead7be54dbc053
3ff9ba6f8008cacc89d36867e769533484a53b59fd74ecafeb2ead7be54dbc054
```

The final block of the contest, block 668293, was mined on 12-31-2020 23:59 (UTC). Block 668293 has the block hash:

```
000000000000000001a900f2cf1fa547caafdfd63a2bf8bd4ccb173cd3a1860f
```

Each ticket is concatenated with the block hash. Thus, the 8 tickets, after being concatenated with the block hash, are:

```
9d055e4a49bea54f2733758377a65169f4f8b50a4984272daa927b10027b20df00
00000000000000001a900f2cf1fa547caafdfd63a2bf8bd4ccb173cd3a1860f
d2b4f0aeb943df16f538a714b10457938cc38d3906b1bed8e5cb953bfd13cde2000
0000000000000001a900f2cf1fa547caafdfd63a2bf8bd4ccb173cd3a1860f
d2b4f0aeb943df16f538a714b10457938cc38d3906b1bed8e5cb953bfd13cde2100
0000000000000001a900f2cf1fa547caafdfd63a2bf8bd4ccb173cd3a1860f
3ff9ba6f8008cacc89d36867e769533484a53b59fd74ecafeb2ead7be54dbc05000
0000000000000001a900f2cf1fa547caafdfd63a2bf8bd4ccb173cd3a1860f
```

```
3ff9ba6f8008cacc89d36867e769533484a53b59fd74ecafeb2ead7be54dbc05100
0000000000000001a900f2cf1fa547caafdfd63a2bf8bd4ccb173cd3a1860f
3ff9ba6f8008cacc89d36867e769533484a53b59fd74ecafeb2ead7be54dbc05200
0000000000000001a900f2cf1fa547caafdfd63a2bf8bd4ccb173cd3a1860f
3ff9ba6f8008cacc89d36867e769533484a53b59fd74ecafeb2ead7be54dbc05300
0000000000000001a900f2cf1fa547caafdfd63a2bf8bd4ccb173cd3a1860f
3ff9ba6f8008cacc89d36867e769533484a53b59fd74ecafeb2ead7be54dbc05400
0000000000000001a900f2cf1fa547caafdfd63a2bf8bd4ccb173cd3a1860f
```

All of these concatenated strings are hashed with the SHA-256 function. The resulting strings are:

```
418df7b64613e5a77ca95a196bff92db095307627c2eaab1f6b6456b333183bb
2ea6c2942dbf3c0c340e87b37689c4f7e405c6113f168c99d22e12a2bb44d022
b846818d41ebc57a3bb0f31d4dfe8712138e7c2c66c6684baaf3eb61f8e367a2
034bb90d821292e90719cb7e9a54d34f0840087d6cea370fd415b9ff4419a7a6
d9ce25a425d3f97e1448ac928fc3179f9ce01e1d6b8bfd1eed2af63fdcc3e2d2
9ac8dd5a1e99b7363a94bf6aa294c19fe41e1a589ff34d476420bb1eba6b7434
da4da7d2a0a887d0c7d14a8670abc358f46866179df3958cfb4d692b6ce28547
ff46a9f04cc355744b96866b2961e1cf55bc0560b60db74a0666d406923e2e71
```

The lowest alphanumeric value out of that list is:

```
034bb90d821292e90719cb7e9a54d34f0840087d6cea370fd415b9ff4419a7a6
```

That string is the SHA-256 result of the concatenated ticket:

```
3ff9ba6f8008cacc89d36867e769533484a53b59fd74ecafeb2ead7be54dbc05000
0000000000000001a900f2cf1fa547caafdfd63a2bf8bd4ccb173cd3a1860f
```

That ticket is derived from the TXID:

```
3ff9ba6f8008cacc89d36867e769533484a53b59fd74ecafeb2ead7be54dbc05
```

The winnings awarded to the entrant that purchased that ticket are sent to the input 0 address from the purchasing transaction, which is qzvqtrrzhgtj0mmyrh923dnlzx60fz75ku5g57akup.