

Vanity Voting: Decentralized Blockchain Voting

aka CryptoVoter

“Smokeasy”

digital.smokeasy@gmail.com

blockchainvoter.com

Abstract. A trustless, decentralized, peer-to-peer (P2P) voting system achieved through voter generated probabilistic vanity cryptocurrency addresses leveraged on any blockchain.

I. Characteristics:

- Decentralized (p2p)
- Zero-trust (users retain complete control over 100% of their coins)
- Based on Bitcoin blockchain technology
- Pseudo-anonymous
- Transparent
- Non-binding
- Auditable
- Resists double-spends (double-votes)
- One-Coin-One-Vote (as opposed to one-person-one-vote)
- Compatible with proxy voting pools

II. Summary of System

Vanity Voting is a decentralized voting system that allows decentralized, trustless voting using end-user generated vanity coin addresses, where total votes cast equals total coins sent to each voter's self-controlled "vanity-voting address."

1. Each answer choice is associated with a unique 6-letter “voting-address prefix.”
2. The question, possible answer choices (w/ corresponding “voting-address prefixes) and a blockheight-deadline (+ n confirmations) are publicly posted.
3. Before voting, each voting coinholder creates a unique, self-controlled “vanity-voting address” where the first 6-bits of said generated address match the posted 6-letter “voting-address prefix” corresponding to their desired vote choice.

4. During the voting period, each voting coinholder sends as many coins as they can/want to their self-controlled “vanity-voting address” until the blockheight-deadline (+ n confirmations) has passed.
5. At the blockheight-deadline (+ n confirmations), address balances for all addresses matching the applicable “voting-address prefixes” and meeting confirmation requirements are tallied and compared to determine the winner.

III. Proof-of-Concept: *Vanity Voting* Example

· An *Easy Vanity Voting* question has 3 parts: (1) the question, (2) potential answer choices and (3) Blockheight deadline (+ n confirmation).

· For this example, we have 31 users using 100 coins to vote on a question 11 with 6 possible answers (100 coins were used to have round numbers).

Question 11: What type of mining equipment should the proof-of-work mining algorithm focus on?

- 1Q11AA – CPU's
- 1Q11BB – Abaci's
- 1Q11CC – FPGA's
- 1Q11DD – GPU's
- 1Q11EE – ASIC's
- 1Q11ZZ – None of the above or Protest vote

Blockheight deadline: 72800 + 30 confirmations

IV. Proof-of-Concept: *Vanity Voting* Results

By visiting <http://btcs-voter.com> we get the following results:

· 1Q11AA Addresses (“CPU's”)
§ 4 addresses contain 5% of total coins voted
§ BALANCE ADDRESS

§ 01.00 BTC 1Q11AA7TJr2k24F59EfcYYQFUvmuuNreiu
§ 00.50 BTC 1Q11AABZuFtkd7Xm9CELB363bqemRsyiVB
§ 02.50 BTC 1Q11AAJqmvSBC41wqAZmreU1QnWN6W69m9
§ 01.00 BTC 1Q11AAhhxap3Sv1CcQJHcTEeCodngVpExi

· 1Q11BB Addresses (“Abaci's”)

§ 3 addresses contain 1.1% of total coins voted

§ BALANCE ADDRESS

§ 00.10 BTC 1Q11BB9xfyqsfchkRxyBGxheaT81bGA26
§ 00.20 BTC 1Q11BBXHpLCGEETKgYYvGJzMNEgxjUxBJZ
§ 00.80 BTC 1Q11BBtz8aCtUX8bek3T6RGjWcfP9My5FV

· 1Q11CC Addresses (“FPGA's”)

§ 6 addresses contain 5.75% of total coins voted

§ BALANCE ADDRESS

§ 02.00 BTC 1Q11CC2Co1Ng2F42NET5WL26NkKGt2WRZB
§ 01.00 BTC 1Q11CCEBoU3Hc2Q9fe3kaf1VQjhjN3WfEX
§ 00.25 BTC 1Q11CCWxcRhWLAhjbdaHXnXDdxX1GnAGvq
§ 01.00 BTC 1Q11CCZa6quv3woAf8HmvcQTs7LZbWLSLq
§ 01.00 BTC 1Q11CCbdeqrb8GJeL14vQsbYyQ4iHJZJZr
§ 00.50 BTC 1Q11CCwubn6xDisbUqE5pcRjntk8oNMbT3

· 1Q11DD Addresses (“GPU's”)

§ 6 addresses contain 51% of total coins voted

§ BALANCE ADDRESS

§ 02.10 BTC 1Q11DD9tM4BpYF1cLLxn39D1hUuXca9acQ
§ 07.20 BTC 1Q11DDSsT2Wt7t3hkoSL8jT83U2qzaZUL8
§ 10.40 BTC 1Q11DDcD6YfJKSy1PHpzseTS7XxkNUKWGP
§ 01.30 BTC 1Q11DDhPtFF5a5n9MgqxcbBQYWcJZk9N77
§ 15.00 BTC 1Q11DDv5fMun6M2ESJ66WjaUjCvokvyYbu
§ 15.00 BTC 1Q11DDvs3k5ZS5SAe2KxtZNPfHVDfHEeX98

· 1Q11EE Addresses (“ASIC's”)

§ 4 addresses contain 9.9% of total coins voted

§ BALANCE ADDRESS

§ 03.00 BTC 1Q11EET2S33rWskCX1eD8nNWgvHPAhYfYJ
§ 03.00 BTC 1Q11EEX4bjnoE8rJjSr9HSaMx7VNbtBaKY
§ 00.90 BTC 1Q11EEw9yXmeKJSBHUb8h6BWxcSAVbrUmr

§ 03.00 BTC 1Q11EEyj8LHmmZcfbP8c3eopUaveP6jDTi

· 1Q11ZZ Addresses (“None of the above or Protest vote”)

§ 8 addresses contain 27.25% of total coins voted

§ BALANCE ADDRESS

§ 15.00 BTC 1Q11ZZ5E7UYFg39BTJSRFRsnhVWGFwEtH9

§ 00.40 BTC 1Q11ZZJkihRp5nJBsxRnkUmgoP7zX3vrLQ

§ 00.10 BTC 1Q11ZZQRtSbSQmFPwWMASCEtxtnp43u18j

§ 00.90 BTC 1Q11ZZZ6UrzwwnxNa4YvA9jTTjWgdWEYrx

§ 09.25 BTC 1Q11ZZenC9UfpbhSnFZjuimGbduBRmJsE9

§ 00.25 BTC 1Q11ZZoA3KFSx8twAxjZLi2cdjN2PDfw3i

§ 00.60 BTC 1Q11ZZsd5EEEnKQJk2JcEyAvjh8DTQ2WMh

§ 00.75 BTC 1Q11ZZsvC1CFyMXy7Tu5DYnpz2BsJLLqcL

Thus, we have the following results:

Question 11 Results: What type of mining equipment should the proof-of-work mining algorithm focus on?

[05.00%] 1Q11AA – CPU's

[01.10%] 1Q11BB – Abaci's

[05.75%] 1Q11CC – FPGA's

[51.00%] 1Q11DD – GPU's <----- Winner

[09.90%] 1Q11EE – ASIC's

[27.25%] 1Q11ZZ – None of the above or Protest vote

[Blockheight deadline: 72800 + 30 confirmations]

Results

Total Votes:100

Answer prefix AA total percent = 5%

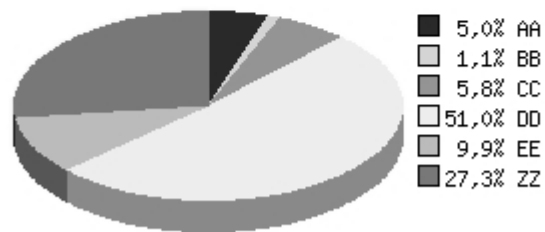
Answer prefix BB total percent = 1.1%

Answer prefix CC total percent = 5.75%

Answer prefix DD total percent = 51%

Answer prefix EE total percent = 9.9%

Answer prefix ZZ total percent = 27.25%



Accordingly, 31 users voted on Question 11 with answer choice DD (GPU's) winning by receiving 51% of total votes cast.