Blind bid protocol v0.21

Dmitry Khovratovich

Dusk Foundation

15th February 2019

1 Notation

Let E be the Bulletproof curve with prime order r.
Variables:

- Seed S – 32-byte string.
- Secret K – 32-byte string.
- Transaction hash X – 32-byte string (?).
- Bidding data M – 32-byte string.
- Merkle tree $\mathcal{T}$ of bids with root R_T.
- Coin amount d – integer between 0 and 2^{64}.
- Counter N – 32-byte string.

Functions:

- H – Longsight, a SNARK-friendly hash function. Defined for 510-bit inputs and 255-bit outputs in a separate file.
- $\mathcal{H}(X, \mathcal{O})$ Merkle root construction function. It assumes that $\mathcal{O}$ is a Merkle opening for X in a tree built using H, and outputs the tree root corresponding to the opening.
- $F(d, Y)$ – score function. Takes 64-bit input d and 256-bit input Y and operates as follows:
  - Truncate Y to left 128 bits and interpret the result as 128-bit integer Y'.
  - Output $f = (d \cdot 2^{128})/Y'$, where division is the integer division.

2 Proof

Let C be the following computation:

- **Public Input:** S.
- **Private Input:** K, d.
- **Flow**
  1. $M = H(K)$;
  2. $Z = H(S, K)$;
  3. $C_d = g^d h^r$
  4. $X = H(C_d, M, S)$;
  5. $\mathcal{H}(X, \mathcal{O}) = R$.
  6. $Y = H(S, X, K)$;
  7. $Q = F(d, Y)$.

  Public Output: Z, R, Q

Then Π is the Bulletproof proof of computational integrity of C.

3 Protocol

Procedure:

1. Seed S is computed and broadcasted.
2. Bidder selects secret K.
3. Bidder, at most once per seed, sends a bidding transaction with data $M = H(K)$ and proof of knowledge of K.
4. For every bidding transaction with d coins in the form of commitment C_d and data M the uniqueness of M is verified and entry $X = H(C_d, M, S)$ is added to $\mathcal{T}$.
5. Potential bidder computes $Y = H(S, X, K)$, score $Q = F(d, Y)$, and identifier $Z = H(S, K)$.
6. Bidder selects a bid root R_T and broadcasts (Z, R_T, Q, π) where

$$\pi = \Pi(Z, R_T, Q, S;\ K, d).$$

7. The proof with the highest Q wins.
8. The winner can use Z to identify himself during the block generation.

4 Security

Requirements:

1. A tuple (Z, R, Q, π) is a proof of knowledge of secret K such that $Z = H(S, K)$.
2. **Bid binding** For given Z it is infeasible to find two different bids that yield the same Z.
3. **Bid privacy** It is infeasible to determine which bidding transaction wins.

Proofs:

1. π is a proof of knowledge of K used in the computation of Z, according to the properties of the Bulletproofs proof system and to the description of computation C.
2. Assuming collision resistance of H it is infeasible to find distinct M, M' giving the same Z or distinct K, K' that ield the same M. Therefore for one Z can exist only one M and one X (by the uniqueness requirement of M), and thus the only possible bid.
3. We prove that the protocol is zero knowledge with respect to the value of winning M. Indeed, each bidding transaction is uniquely identified with M. The privacy of d follows from the facts that C_d has the hiding property and that π is zero knowledge with respect to d.

   Now consider an augmented protocol where the bidder additionally broadcasts d and Y, so the score can be calculated by Verifier and its function F plays no role in the zero-knowledge proof, and neither does R_T. Assuming that H behaves as a random oracle, we see that Z is a randomly generated value for each new seed, whereas π is zero-knowledge by the Bulletproofs security proof. Moreover, as H is preimage-resistant, Verifier can not learn X from Y. Altogether, in this protocol Verifier learns nothing on X nor M.