COMP4901W - Introduction to Blockchain, Cryptocurrencies and Smart Contract Spring 2023

Taught by Amir Gohashady

Notes by Marcus Chan

May 20, 2023

Contents

1 Lecture1

1.1 Properties of hasing:

1. collision-resistant: $h(x) \neq h(y)$ for $x \neq y$
2. hiding: can't find x s.t. $h(x) = y$

1.2 Applications:

1. finding files
2. ledger with pointers
3. commitment scheme

   bidding protocol: for security reasons

   (a) highest bid can be found
   (b) no player can change the bid after seeing others' bid
   (c) auditability (i.e. auditor won't change the deals)

   steps:

   (a) compute $h(b_i + n_i)$ for each player and choose a random number n_i from large domain
   (b) player publishes the hash (commit)
   (c) player publish the bid and n_i for others to hash and verify (reveal)

2 Lecture3

2.1 Merkle tree

Protocol:

1. reclaim once
2. message is short(const)
3. deposit can be taken back
4. message doesnt leak
5. proof p_i is provided and can be decoded