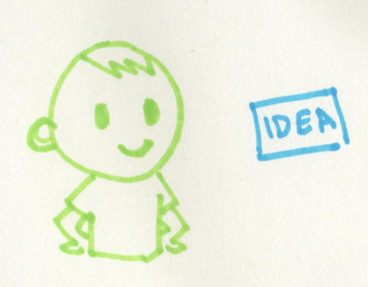
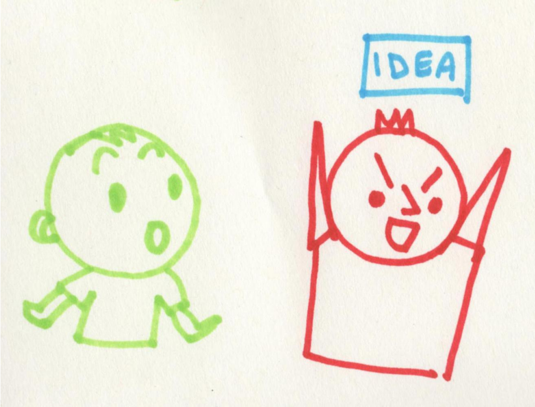
Private Publishing using Bitcoin

Leo Alcock
Mentor: Ling Ren
https://github.com/leoa9001/Private-Publishing

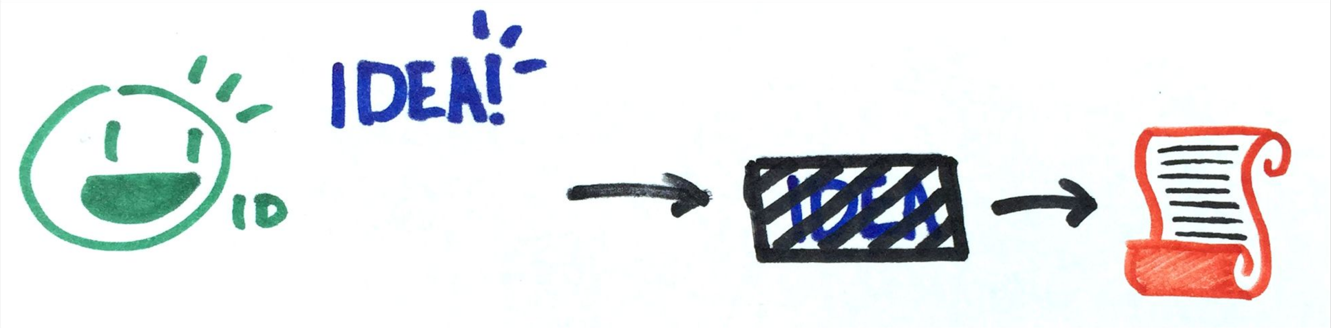
Problem/Application/Motivation

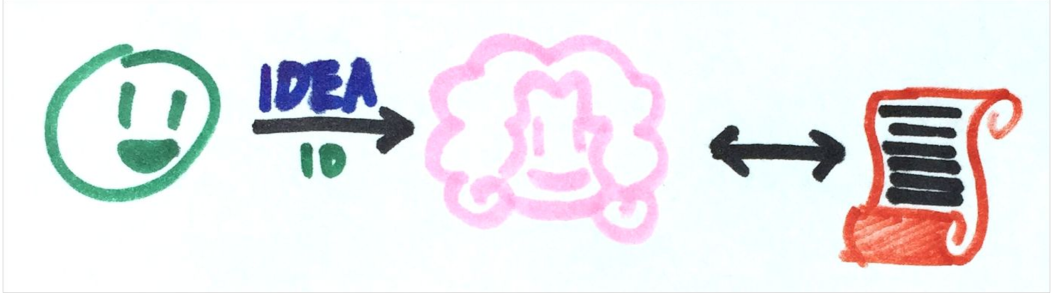
- Prove you have arbitrary data x at time t without revealing any features of data x at time t.





Private Publishing



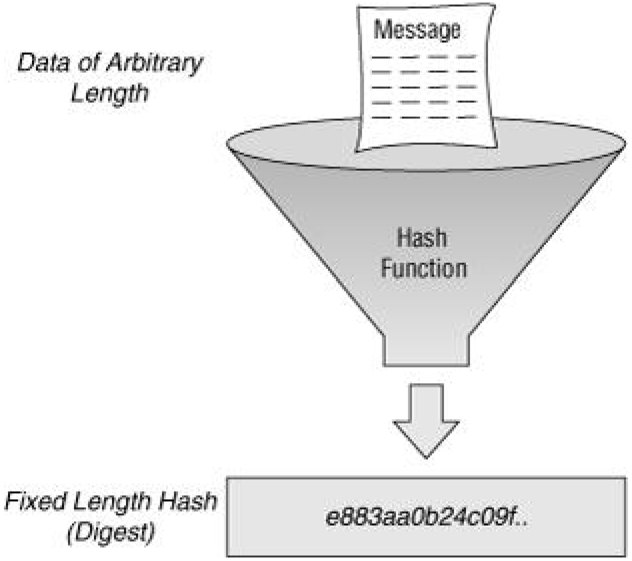


Outline

- Background/Cryptographic Primitives
- Bitcoin
- Implementation Details
- Other works

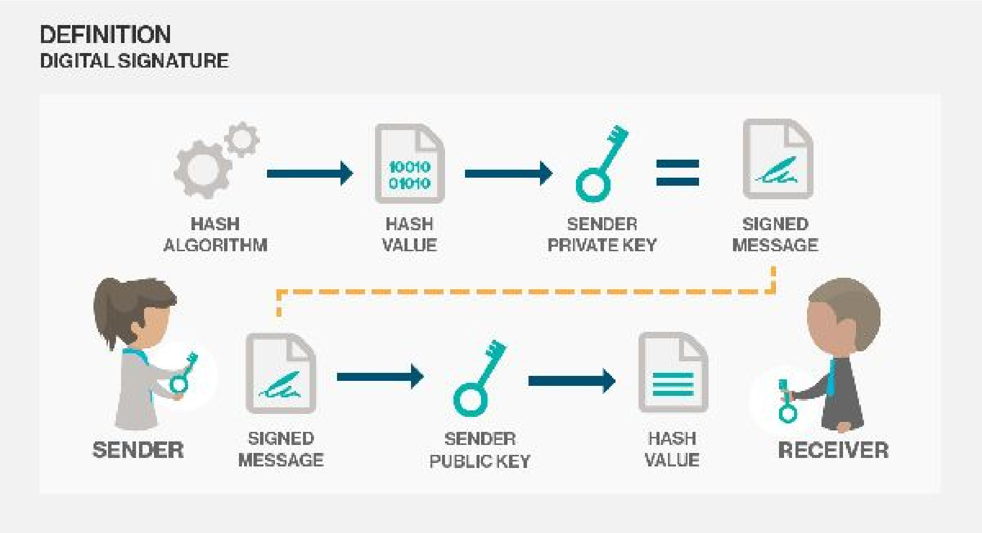
Hashing

- Fast to compute
- Irreversible
- Collision Resistant



Digital Signatures

- Every has user has their own secret key and public key.
- People can “sign” messages using their secret key and then anyone can validate the message’s origin with the public key.
- Hash and private publish the public key with the data

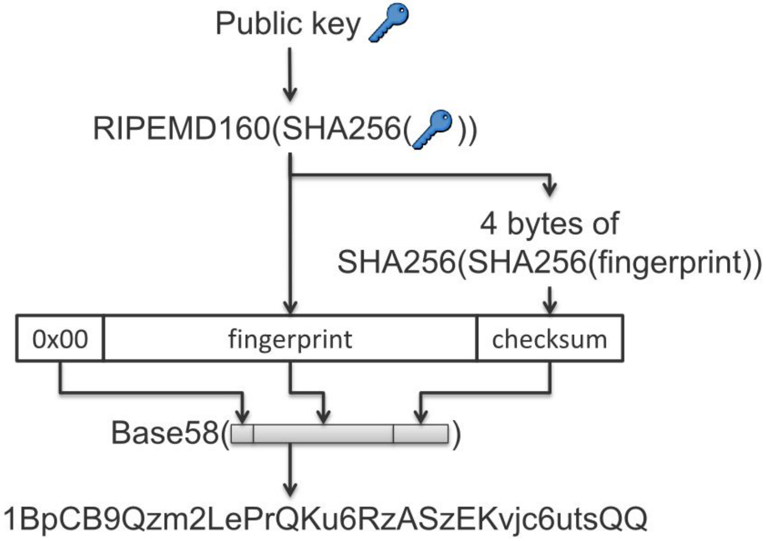


Bitcoin: A Cryptocurrency

- Decentralized Digital Currency
- Transacted directly over the net

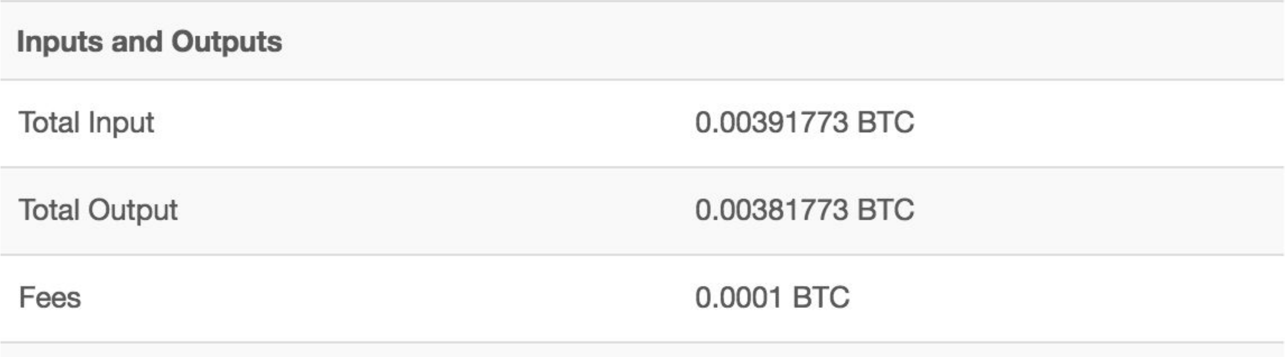
Bitcoin: Address Generation

- People form addresses by generating a key pair and then performing a series of hashes and finally convert into base 58 to make readable.
- Use digital signatures to spend money

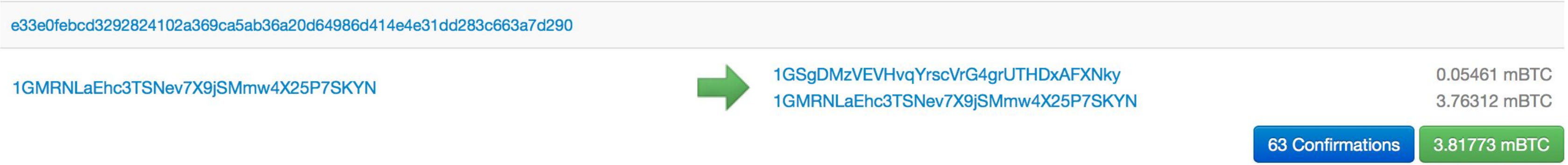


Bitcoin: Transaction Format

- Inputs to send from
- Outputs to send to
- Signed by Secret key



Inputs and Outputs	
Total Input	0.00391773 BTC
Total Output	0.00381773 BTC
Fees	0.0001 BTC



e33e0febcd3292824102a369ca5ab36a20d64986d414e4e31dd283c663a7d290

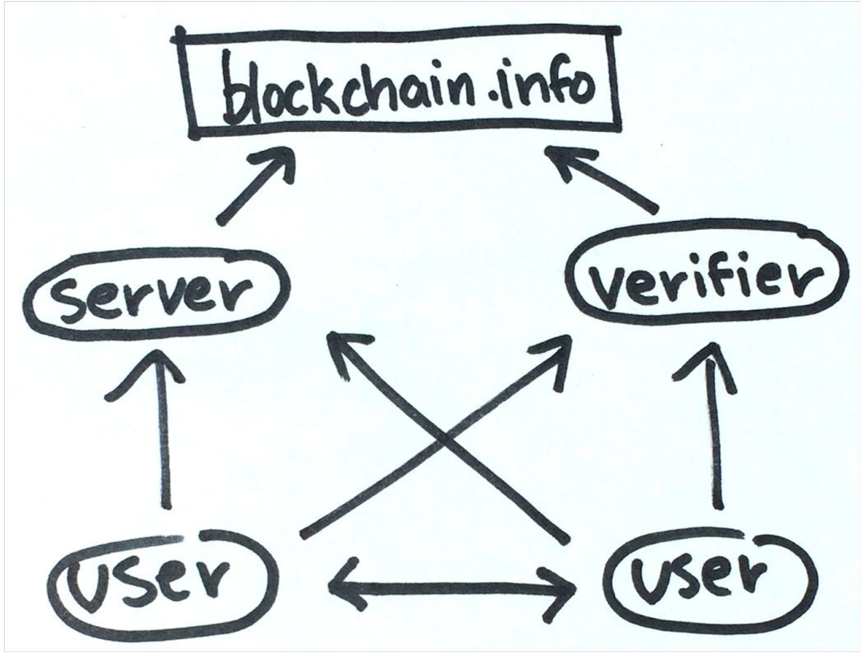
1GMRNLaEhc3TSNev7X9jSMmw4X25P7SKYN → 1GSgDMzVEVHvqYrscVrG4grUTHDxAFXNky 0.05461 mBTC
1GMRNLaEhc3TSNev7X9jSMmw4X25P7SKYN 3.76312 mBTC

Bitcoin: Secure Public Ledger

- Public Ledger held many users
- Transactions are secured to be unchangeable by miners who do proofs of work
- Miners are motivated by block rewards and transaction fees

Implementation Details

- Server-user model



Implementation Details

- Password protected identity using a PRG
- Double hash for server attack

Other works

- Cryptographic Commitment Scheme
- Non-interactive Proofs of Sequential Work
- CommitCoin scheme

Acknowledgements

- My mentor Ling Ren.
- My parents
- MIT PRIMES