mas.s62
lecture 1

2018-02-07

Neha Narula & Tadge Dryja

Primitives for making a cryptocurrency

Hash functions

Signatures

Hash functions

Simple, right? But powerful.

hash(data) -> output

data can be any size; output is fixed size

Hash functions

Important. You can do everything* with just hash functions.

*can’t do some fun stuff with keys

(Key exchange, signature aggregation, etc)

Hash functions

Any size input, fixed output… output is “random” looking

What’s that mean? Deterministic, no randomness

But the outputs look like noise; half the bits are 1s, half are 0s

Hash functions

Somewhat more well defined -

“Avalanche effect”: change 1 bit of the input, about half the output bits should change

Hash functions

Well defined: what it shouldn’t do

preimage resistance

(2nd preimage resistance)

collision resistance

preimage resistance

given y, you can’t find any x such that hash(x) == y

(you can find it eventually, but that will take 2^{256} operations (10^{78}))

2nd preimage resistance

given x, y, such that hash(x) == y, you can’t find x’ where

x’ != x

and hash(x’) == y

(this one is a bit of a mess so lets leave it at that)

collision resistance

nobody can find any x, z such that

x != z

hash(x) == hash(z)

(again, you can find them eventually. And in this case, not 2^{256})

resistances

Practically speaking, collision resistance is “harder”;

collision resistance is broken while preimage resistance remains

Examples: sha-1, md5

usages

hashes are names

hashes are references

hashes are pointers

hashes are commitments

Commit reveal

Commit to something secret by publishing a hash

Reveal the preimage later.

Example: `a1c089bf65e852cf2ba2010d2ba84e2025ec937b5f8b9dac682c35dcf498aef4`

Commit reveal

a1c089bf65e852cf2ba2010d2ba84e2025ec937b5f8b9dac682c35dcf498aef4

Reveal:

I think it won't snow Wednesday! d79fe819

```
$ echo "I think it won't snow Wednesday! d79fe819" | sha256sum

a1c089bf65e852cf2ba2010d2ba84e2025ec937b5f8b9dac682c35dcf498aef4  -
```

Commit reveal

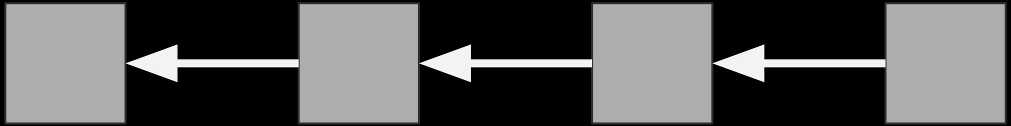
```
$ echo "I think it won't snow Wednesday! d79fe819" | sha256sum

a1c089bf65e852cf2ba2010d2ba84e2025ec937b5f8b9dac682c35dcf498aef4  -
```

Add randomness so people can’t guess my preimage; HMAC

This is a kind of proto-signature

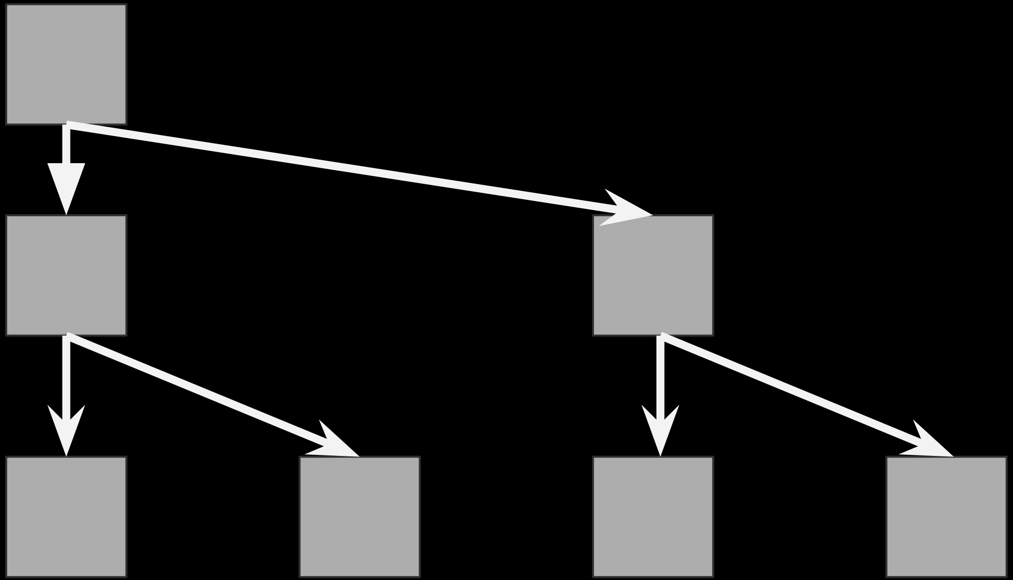
Linked list with hashes



We could call this a “hash-chain”

Also, it’s basically git

Binary tree with hashes



How can 2 inputs go to 1 output?
Not a collision. Concatenate then hash: h(a,b)

What’s a signature?

Signatures are useful! Messages from someone. 3 functions needed:

```
GenerateKeys()

Sign(secretKey, message)

Verify(publicKey, message, signature)
```

3 functions

GenerateKeys()

Returns a privateKey, publicKey pair

Takes in only randomness

3 functions

`Sign(secretKey, message)`

Signs a message given a secretKey.

Returns a signature.

3 functions

```
Verify(publicKey, message, signature)
```

Verify a signature on a message from a public key. Returns a boolean whether it worked or not.

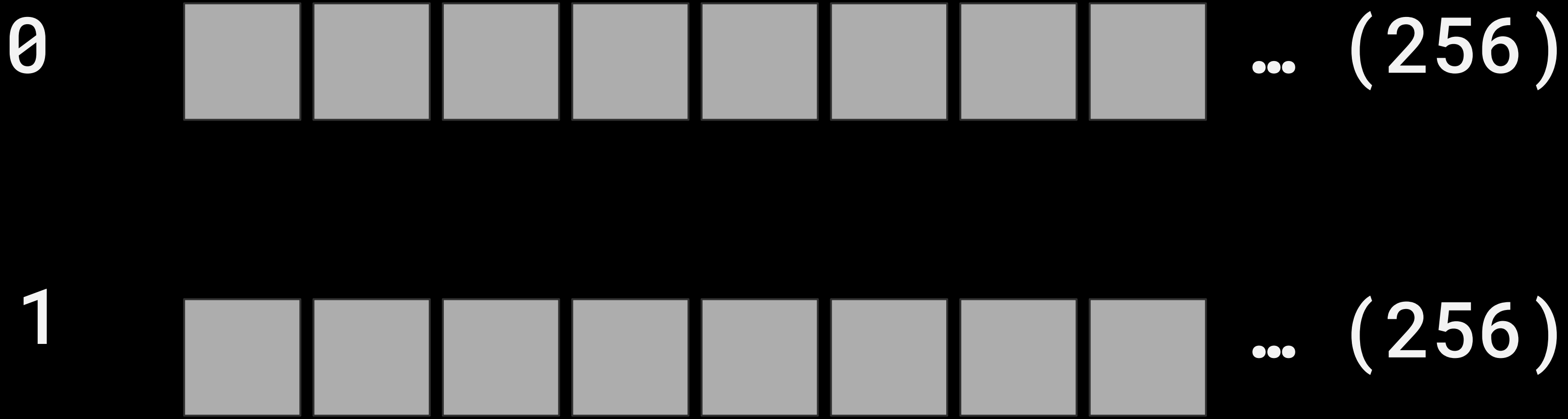
Signatures from hashes

It’s doable! In fact, you’ll do it!

First pset is to implement a signature system using only hashes.

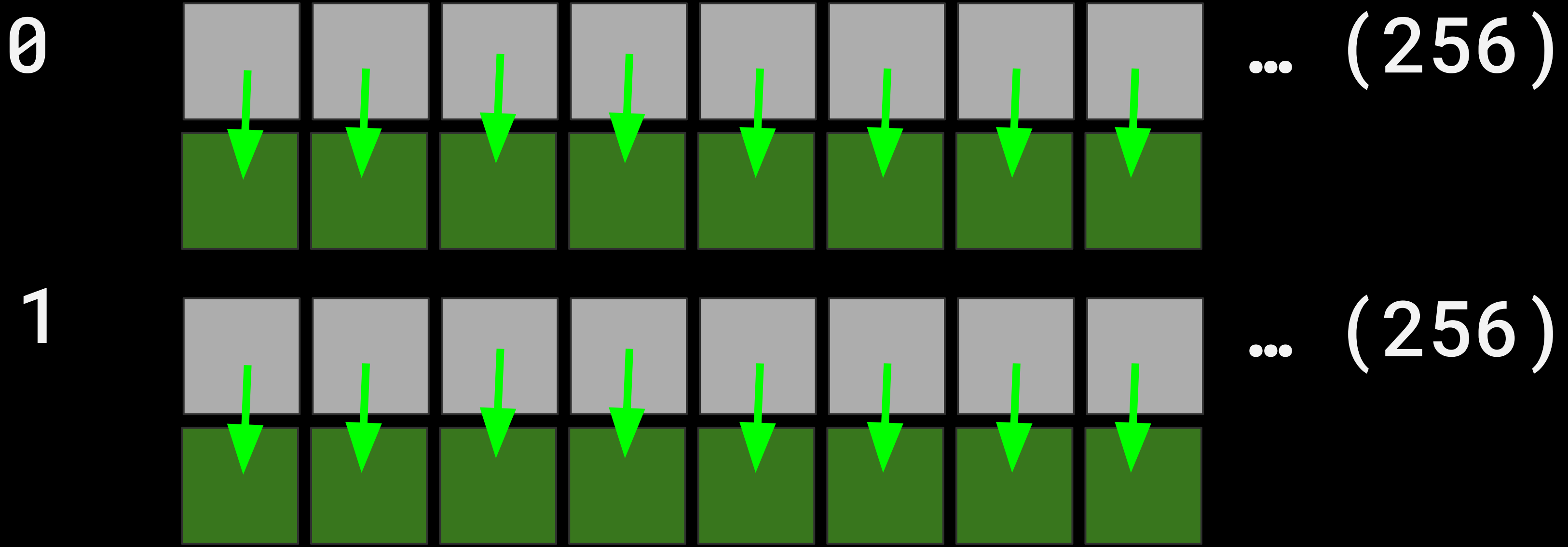
This is called “Lamport Signatures”

Lamport Sigs: Generate key



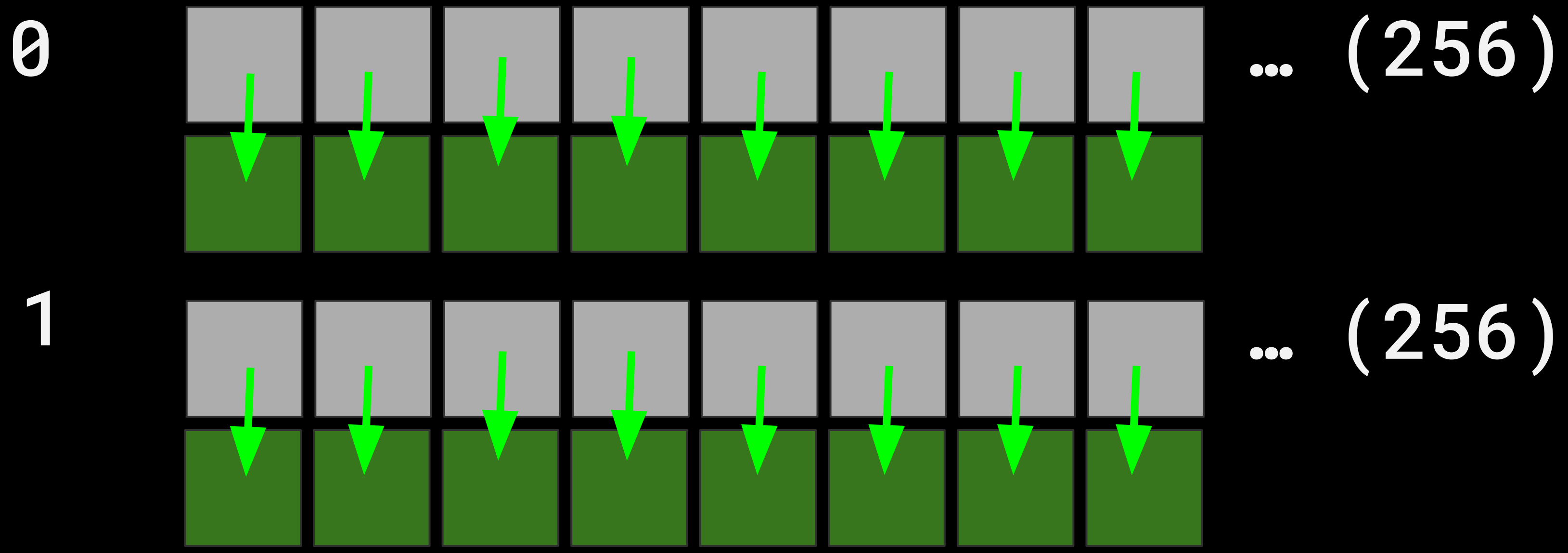
Make up 256*2 random 256 bit numbers

Lamport Sigs: Generate key



Get hashes for each

Lamport Sigs: Generate key



⬜ = Secret key

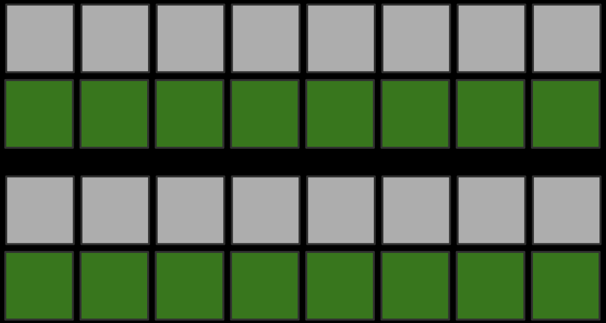
🟩 = public key

Lamport Sigs: Sign

Hash string to sign.

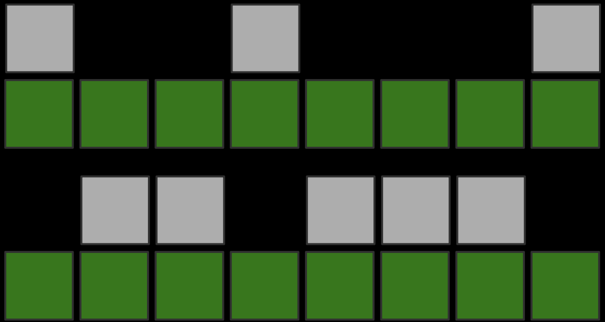
“Hi” = 8f434346648f6b96df89dda901c5176b10a6d83961dd3c1ac88b59b2dc327aa4

Pick private key blocks to reveal based on bits of message to sign



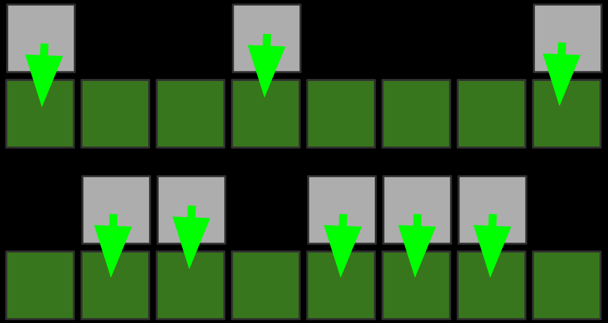
Lamport Sigs: Sign

Hash string to sign.
Pick private key blocks to reveal based on bits of message to sign
01101110



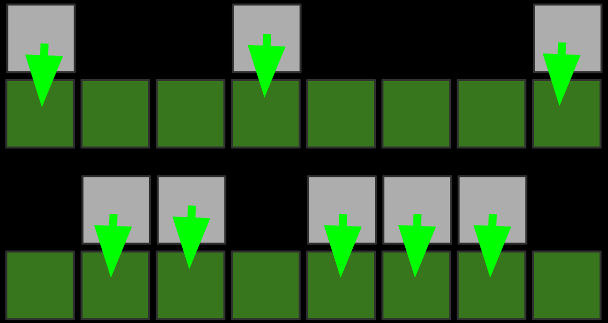
Lamport Sigs: Verify

Hash each block of the signature
Verify that it turns into the block
of the public key



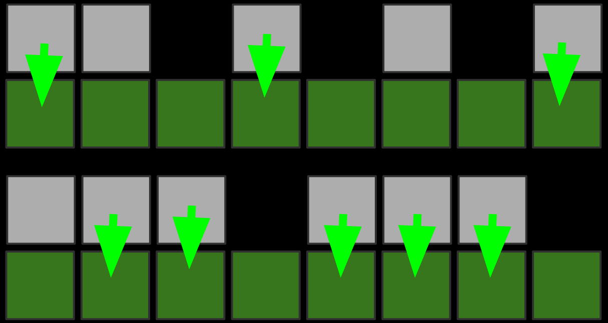
Lamport Sigs: Signing again

Signing more than once reveals more pieces of the private key



Lamport Sigs: Signing again

Signing more than once reveals more pieces of the private key



Lamport Sigs: Signing again

1 sig: can’t forge anything
2 sigs: ~½ bits constrained
3 sigs: ~¼ bits constrained

pset01: Lamport signatures

In golang
On github
Most of the signing code is written
Tests implemented
Also public key with 4 signatures;
try to forge another!
Office hours / messages on slack

pset01: Lamport signatures

github.com/mit-dci/mas.s62

```
$ go get github.com/mit-dci/mas.s62
```

Submissions on github.mit.edu
(procedure not yet finalized)
Office hours Tues 4-6pm
freenode #mass62
mitdci.slack.com #mas-s62
Have fun!

Housekeeping

Signup sheet
Register!
https://github.com/mit-dci/mas.s62
fiorenza@mit.edu to join blockchain lunches, W 11:45 AM in Sloan
Office hours Tues 4-6pm
freenode #mass62
mitdci.slack.com #mas-s62
Have fun!