COS433/Math 473: Cryptography

Mark Zhandry

Princeton University

Fall 2020

Announcements/Reminders

HW6 due Nov 24

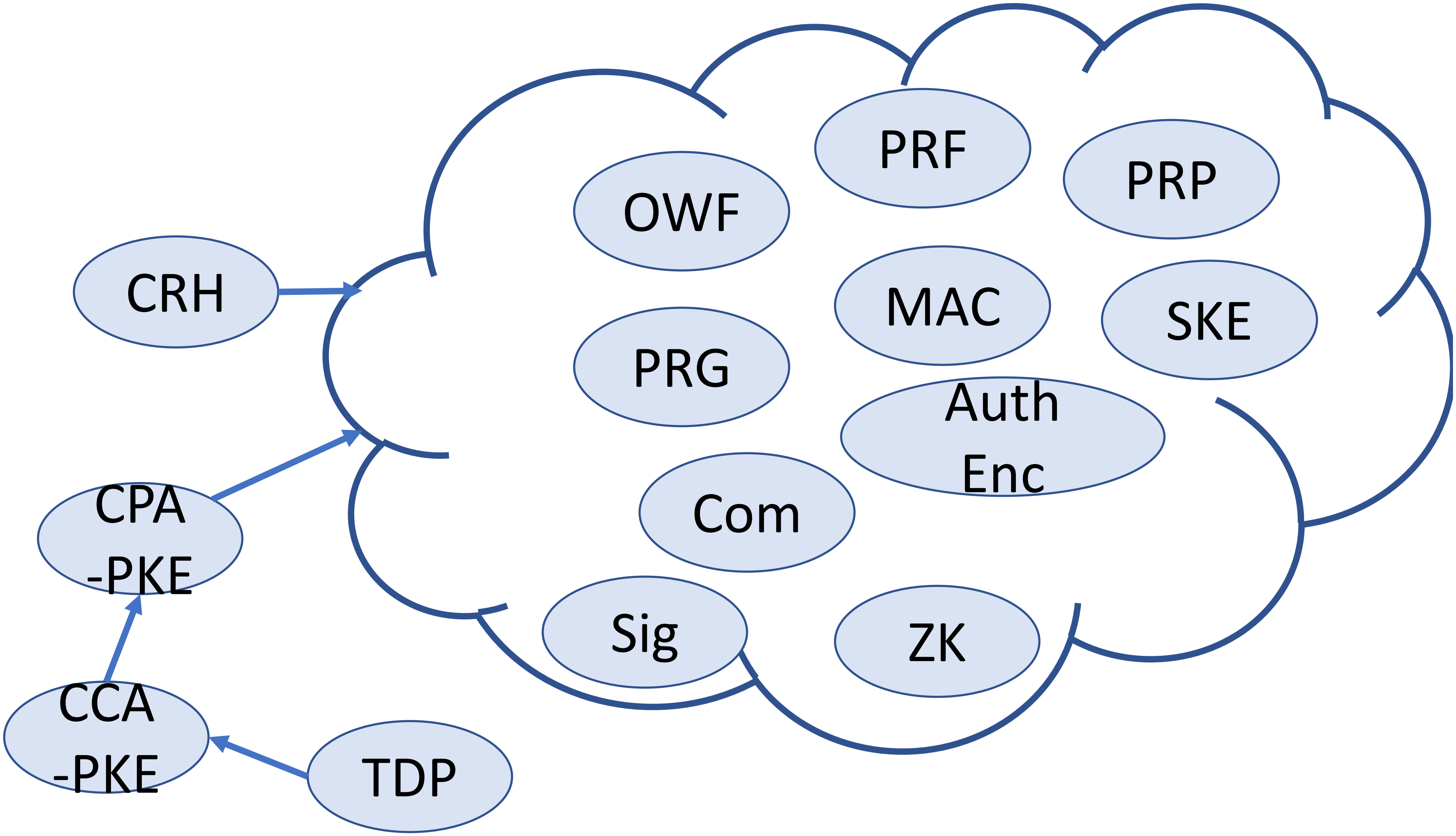
PR2 due Dec 5

No lecture on Thursday (Nov 19)

Previously on COS 433…

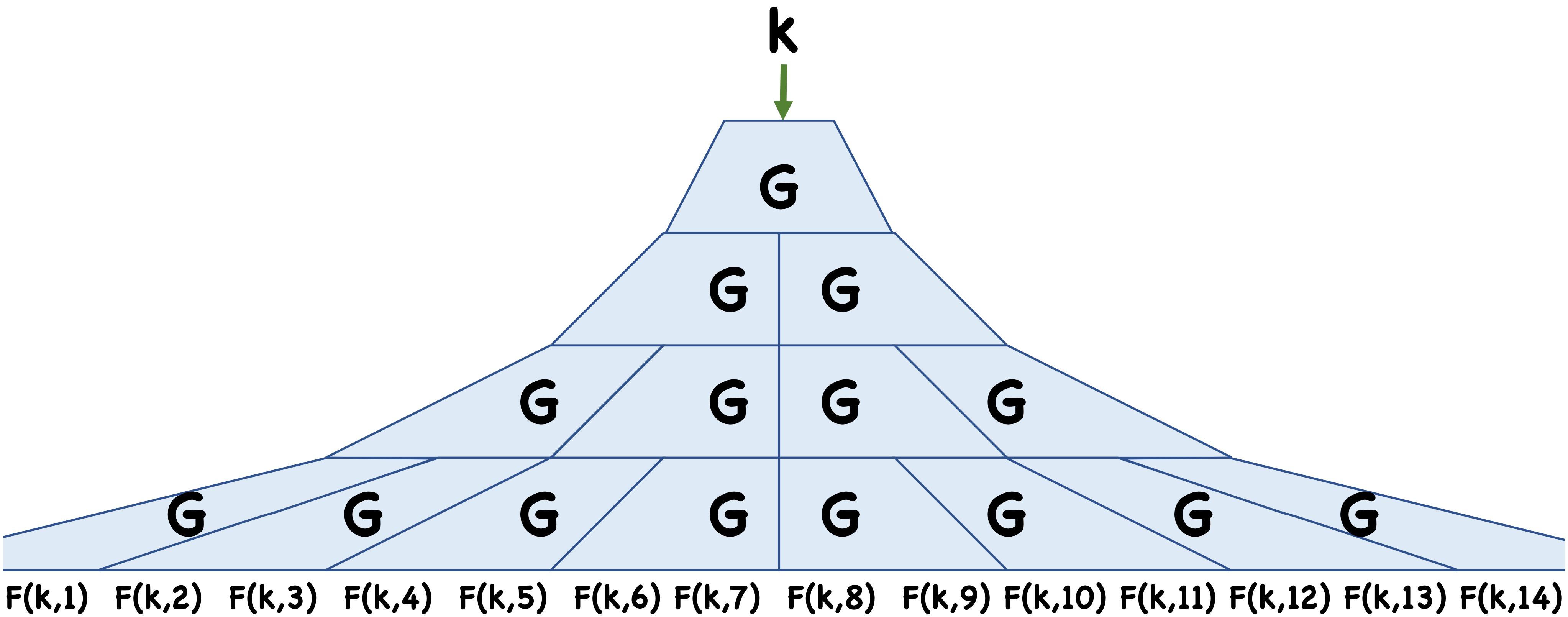
Crypto from Minimal Assumptions

What's Known



CRH
OWF
PRF
PRP
MAC
SKE
PRG
Auth Enc
Com
Sig
ZK
CPA -PKE
CCA -PKE
TDP

A PRF



k
G
G
G
G
G
G
G
G
G
G
G
G
G
G
G
F(k,1)
F(k,2)
F(k,3)
F(k,4)
F(k,5)
F(k,6)
F(k,7)
F(k,8)
F(k,9)
F(k,10)
F(k,11)
F(k,12)
F(k,13)
F(k,14)

Today

OWP → PRGs
OWF → One-time Signature
Black box separations

If time, cryptocurrencies

One-way *permutation* → PRGs

OWP = OWF that is also a permutation

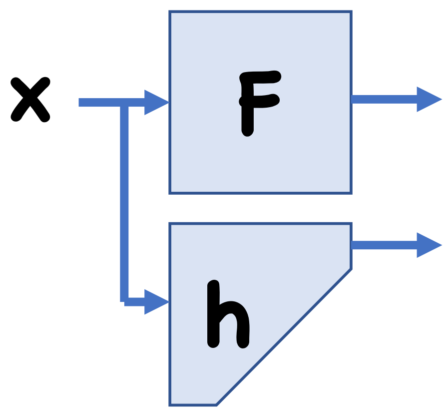
- **F:D→D** is a permutation

Examples:

- RSA function
- Discrete exponentiation

One-way *permutation* → PRGs

Let **h** be a hardcore bit for **F**



Hardcore bit equivalent to PRG security

Hardcore bits for OWPs?

Known OWPs have hardcore bits

- E.g. **LSB, Half** for RSA, **Half** for Dlog

What about general OWPs?

Yao's Method

Let **F** be a OWP with domain $\{0,1\}^n$

Claim: $\exists$ **i** such that $\forall$ PPT **A**

$$\Pr[A(F(x)) = x_i] < 1 - 1/2n$$

Proof: otherwise, $\forall$ **i**, $\exists A_i$ **s.t.**

$$\Pr[A_i(F(x)) = x_i] \geq 1 - 1/2n$$

Adversary $A(y) = A_1(y) || A_2(y) || \ldots$

$$\Pr[A(F(x)) = x] \geq 1/2$$

Yao's Method

Let **F** be a OWP with domain $\{0,1\}^n$

Claim: $\exists$ **i** such that $\forall$ PPT **A**

$$\Pr[A(F(x)) = x_i] < 1 - 1/2n$$

Let $F'(x^{(1)},\ldots,x^{(t)}) = (F(x^{(1)}),\ldots,F(x^{(t)}))$

$$h(x^{(1)},\ldots,x^{(t)}) = x^{(1)}_i \oplus x^{(2)}_i \oplus \ldots \oplus x^{(t)}_i$$

Yao's XOR lemma $\Rightarrow$ **h** is hardcore for **F'**

Goldreich Levin

Let $\mathbf{F}$ be a OWP with domain $\{0,1\}^n$ and range Y

Let $F':\{0,1\}^{2n} \rightarrow \{0,1\}^n \times Y$ be:

$$F'(r,x) = r,F(x)$$

Define $h(r,x) = \langle r,x \rangle = \Sigma r_i x_i \bmod 2$

Theorem (Goldreich-Levin): If $\mathbf{F}$ is one-way, then $\mathbf{h}$ is a hc bit for $\mathbf{F'}$

OWF → PRGs

Yao, Goldreich-Levin also work for general OWFs

However, **(F(x),h(x))** may not be a PRG for a general OWF

- Output may be shorter than input
- **F** may be biased

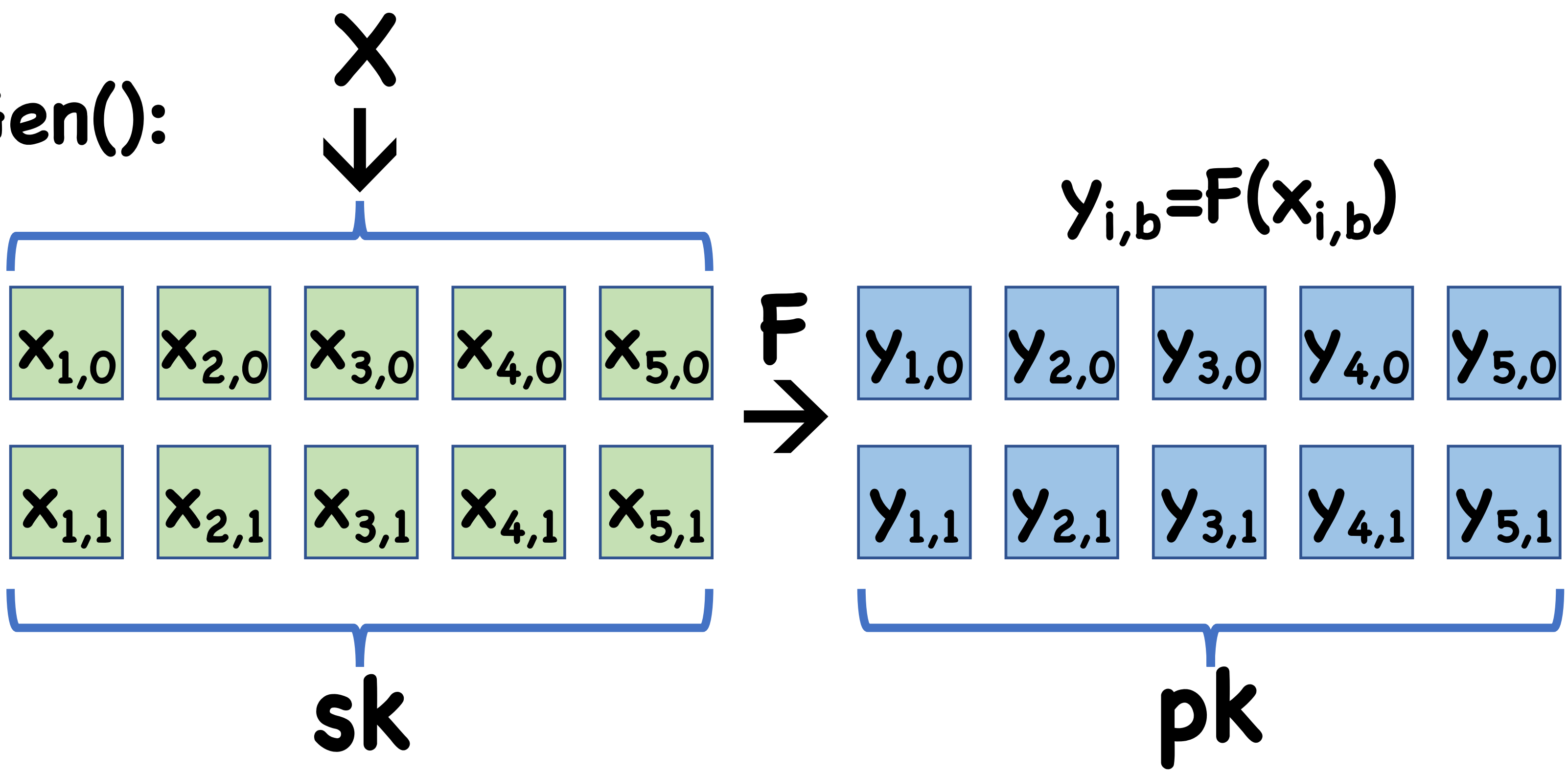
With some effort, can build PRF from any one-way function using similar ideas

Lamport Signatures

Let **F:X→Y** be a one-way function

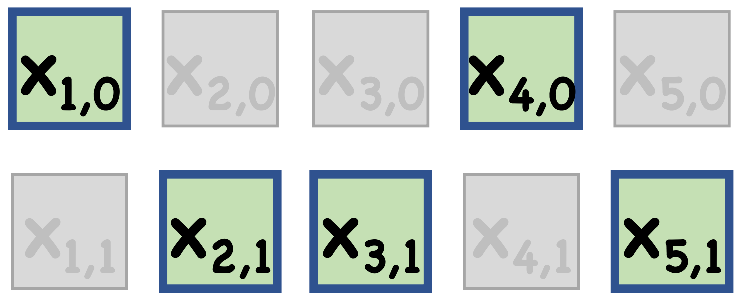
Let $\mathbf{M=\{0,1\}^n}$ be message space

Gen():

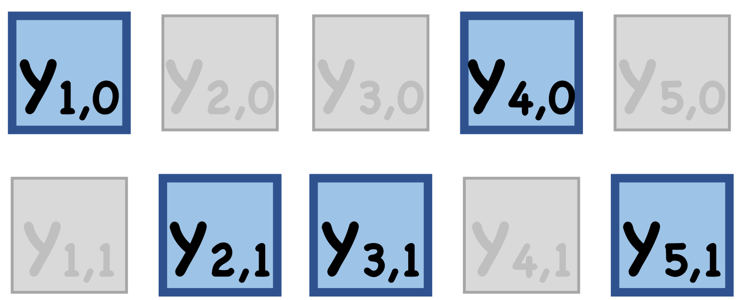


Lamport Signatures

Sign(sk, m): $(x_{i,m_i})_{i=1,\dots,n}$



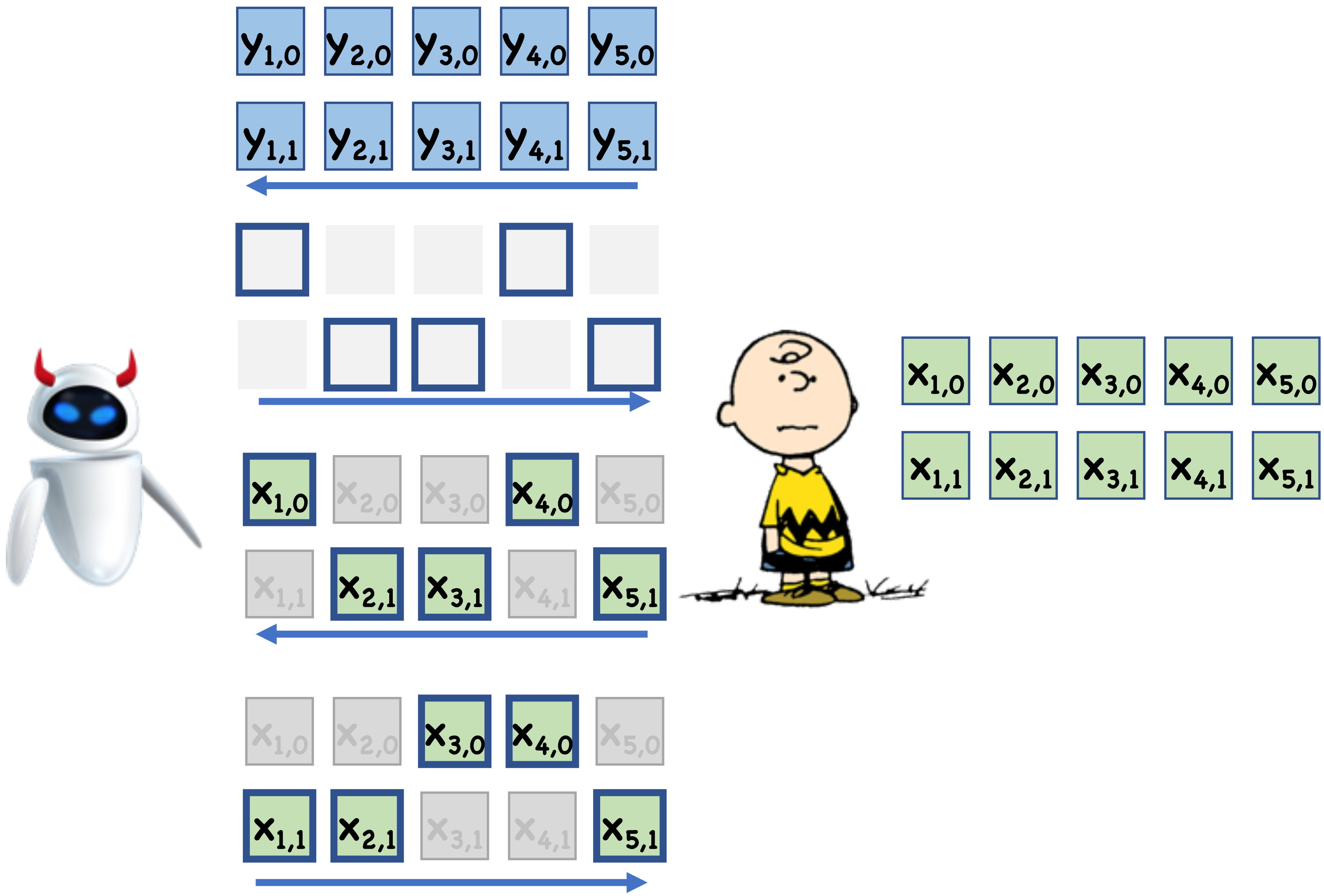
Ver(pk,m,σ): $F(x_{i,m_i}) = y_{i,m_i}$



Lamport Signatures

Theorem: If **F** is a secure OWF, then **(Gen,Sign,Ver)** is a (weakly) secure one-time signature scheme

Proof



$y_{1,0}$ $y_{2,0}$ $y_{3,0}$ $y_{4,0}$ $y_{5,0}$
$y_{1,1}$ $y_{2,1}$ $y_{3,1}$ $y_{4,1}$ $y_{5,1}$
$x_{1,0}$ $x_{2,0}$ $x_{3,0}$ $x_{4,0}$ $x_{5,0}$
$x_{1,1}$ $x_{2,1}$ $x_{3,1}$ $x_{4,1}$ $x_{5,1}$
$x_{1,0}$ $x_{2,0}$ $x_{3,0}$ $x_{4,0}$ $x_{5,0}$
$x_{1,1}$ $x_{2,1}$ $x_{3,1}$ $x_{4,1}$ $x_{5,1}$
$x_{1,0}$ $x_{2,0}$ $x_{3,0}$ $x_{4,0}$ $x_{5,0}$
$x_{1,1}$ $x_{2,1}$ $x_{3,1}$ $x_{4,1}$ $x_{5,1}$

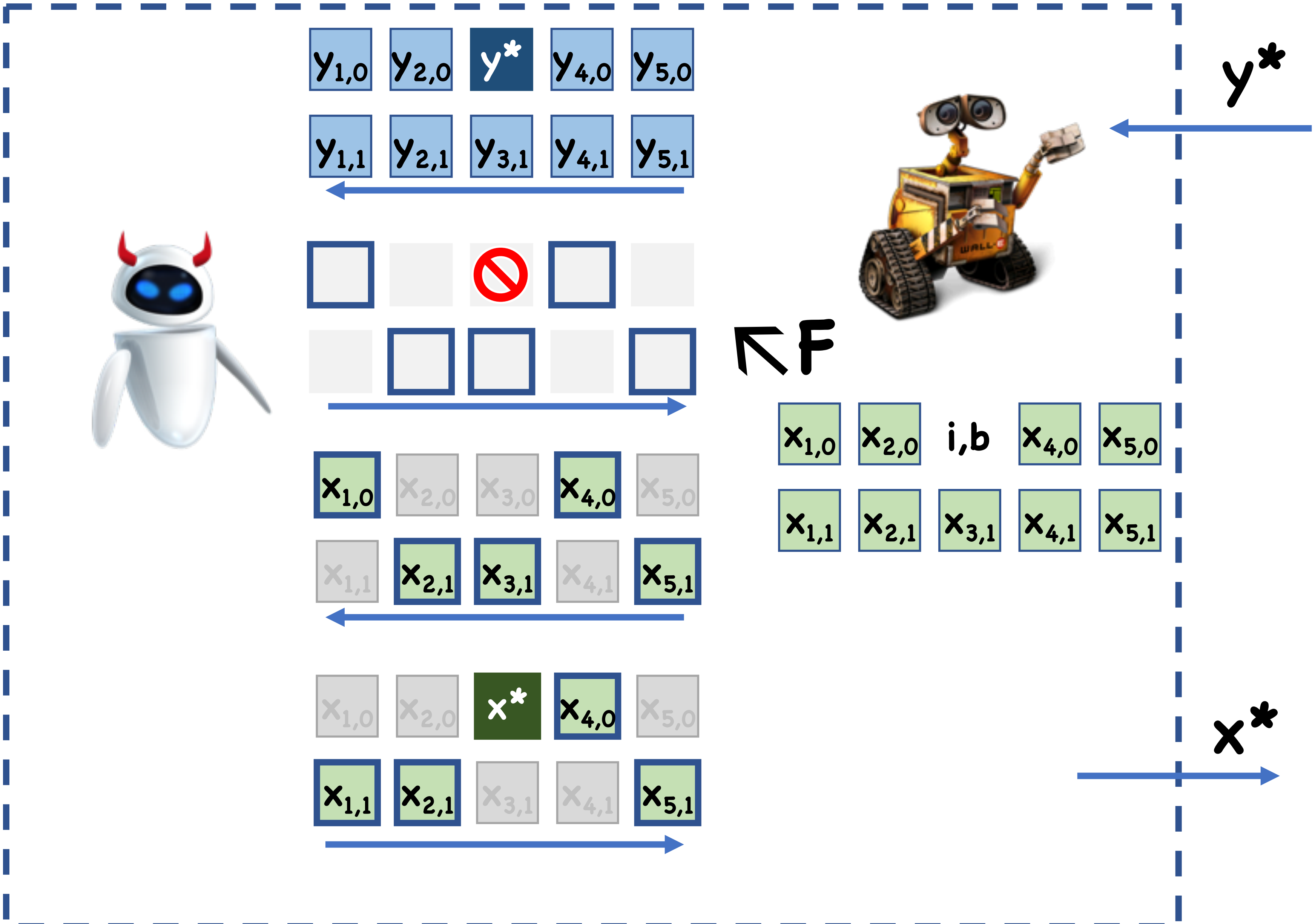
Proof

Since $m^* \neq m$, $\exists i$ s.t. $m^*_i \neq m_i$

Suppose we know i, $m_i = 1-b$, $m^*_i = b$

Construct adversary that inverts OWF

Proof



y1,0 y2,0 y* y4,0 y5,0
y1,1 y2,1 y3,1 y4,1 y5,1
y*
F
x1,0 x2,0 i,b x4,0 x5,0
x1,1 x2,1 x3,1 x4,1 x5,1
x1,0 x2,0 x3,0 x4,0 x5,0
x1,1 x2,1 x3,1 x4,1 x5,1
x1,0 x2,0 x* x4,0 x5,0
x1,1 x2,1 x3,1 x4,1 x5,1
x*

Proof

View of  exactly as in 1-time CMA experiment, assuming

- **i**th bit of **m = b**
- **i**th bit of **m* = 1-b**

If  always chooses **m,m*** with these properties, and forges with probability **ε**, then  inverts with probability **ε**

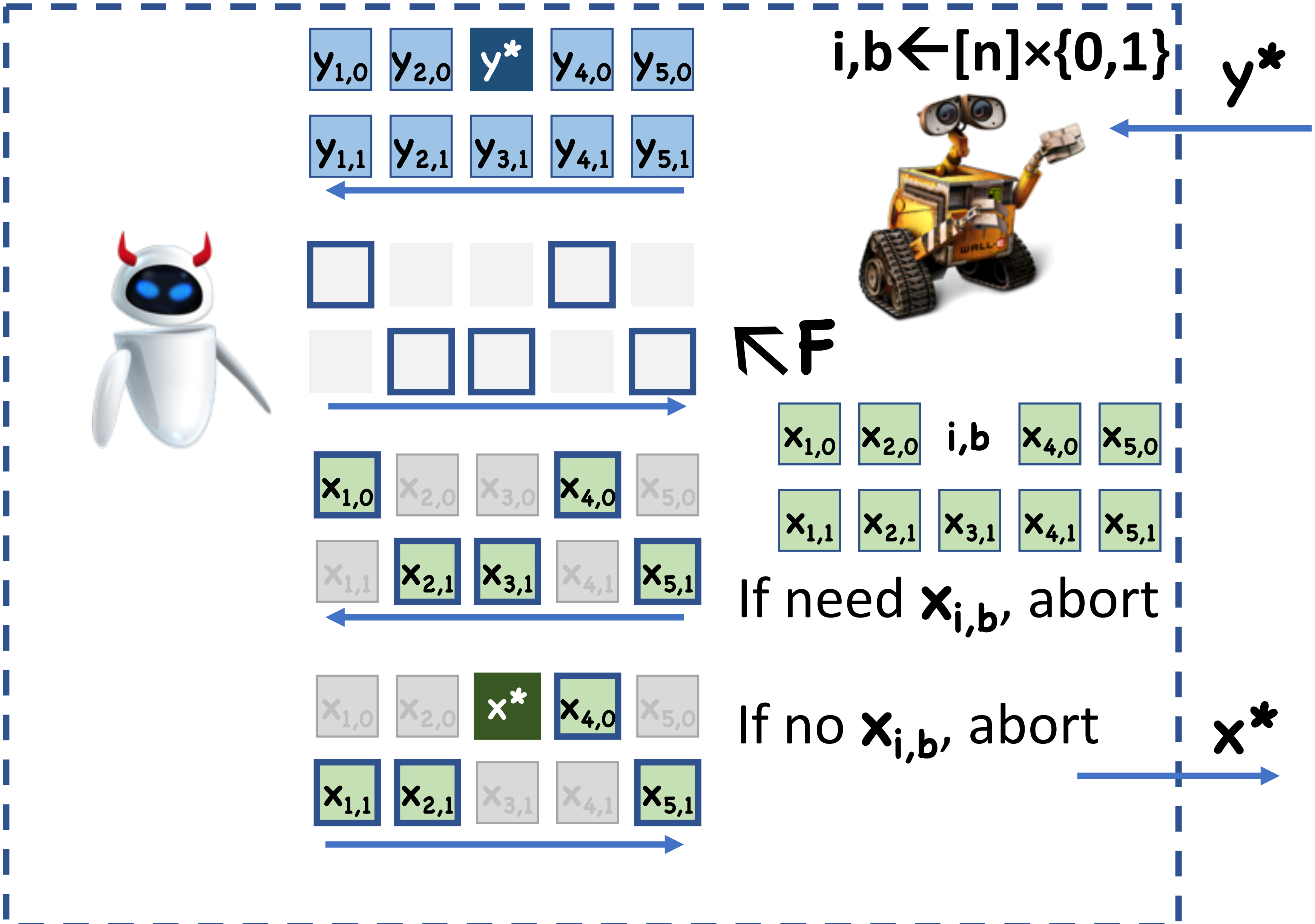
Proof

In general,  may choose **m,m*** to differ at arbitrary places

- May be randomly chosen, may depend on **pk**, may even depend on **σ**
- May never be at certain places

How do we make  still succeed?

Proof



$y_{1,0}$ $y_{2,0}$ y^* $y_{4,0}$ $y_{5,0}$
$y_{1,1}$ $y_{2,1}$ $y_{3,1}$ $y_{4,1}$ $y_{5,1}$
$i,b \leftarrow [n]\times\{0,1\}$
y^*
$\leftarrow F$
$x_{1,0}$ $x_{2,0}$ i,b $x_{4,0}$ $x_{5,0}$
$x_{1,1}$ $x_{2,1}$ $x_{3,1}$ $x_{4,1}$ $x_{5,1}$
$x_{1,0}$ $x_{2,0}$ $x_{3,0}$ $x_{4,0}$ $x_{5,0}$
$x_{1,1}$ $x_{2,1}$ $x_{3,1}$ $x_{4,1}$ $x_{5,1}$
If need $x_{i,b}$, abort
$x_{1,0}$ $x_{2,0}$ x^* $x_{4,0}$ $x_{5,0}$
$x_{1,1}$ $x_{2,1}$ $x_{3,1}$ $x_{4,1}$ $x_{5,1}$
If no $x_{i,b}$, abort
x^*

Proof

pk independent of **(i,b)**
- **m** independent of **(i,b)**
- Therefore, $\Pr[m_i=1-b]=½$

Conditioned on $m_i=1-b$,
- Signing succeeds
- **σ** independent of **i**
-  forges with probability **ε**, independent of **i**

Proof

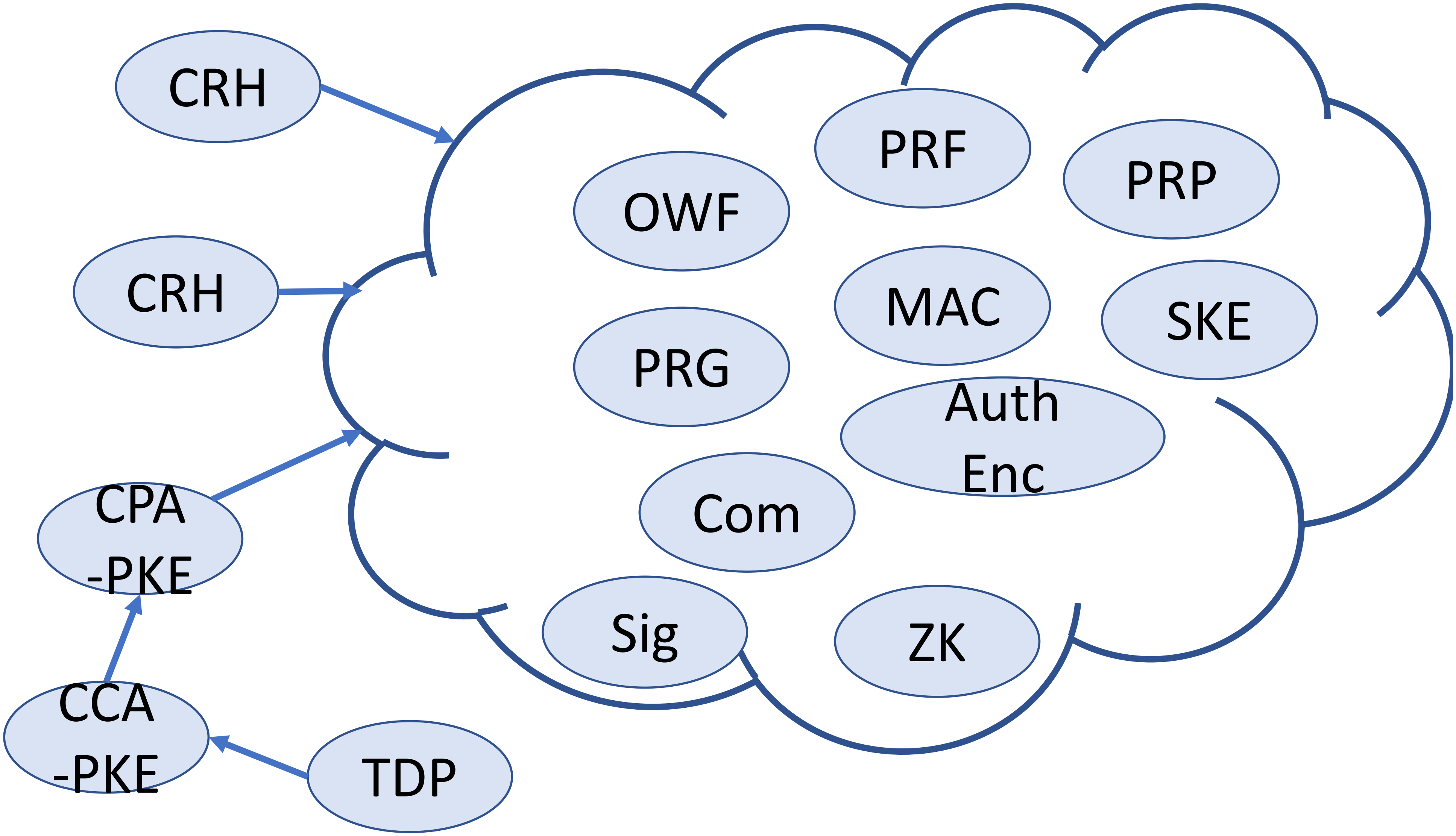
We know if  forges, then $\mathbf{m^* \neq m}$

Since $\mathbf{m^*}$ independent of $\mathbf{i}$, have prob at least $\mathbf{1/n}$ that $\mathbf{m^*_i = 1 - m_i = b}$

In this case,  succeeds in inverting $\mathbf{y^*}$

- Prob = $\frac{1}{2} \times \varepsilon \times 1/n = \varepsilon/2n$

What's Known


CRH
CRH
CPA
-PKE
CCA
-PKE
TDP
OWF
PRG
PRF
PRP
MAC
SKE
Auth
Enc
Com
Sig
ZK

Generally Believed That…

OWF $\not\Rightarrow$ CRHF, OWP, PKE

CRHF $\not\Rightarrow$ OWP, PKE

OWP $\not\Rightarrow$ CRHF, PKE

PKE $\not\Rightarrow$ CRHF

Black Box Separations

How do we argue that you cannot build collision resistance from one-way functions?

- We generally believe both exist!

Observation: most natural constructions treat underlying objects as black boxes (don’t look at code, just input/output)

Maybe we can rule out such natural constructions

Black Box Separations

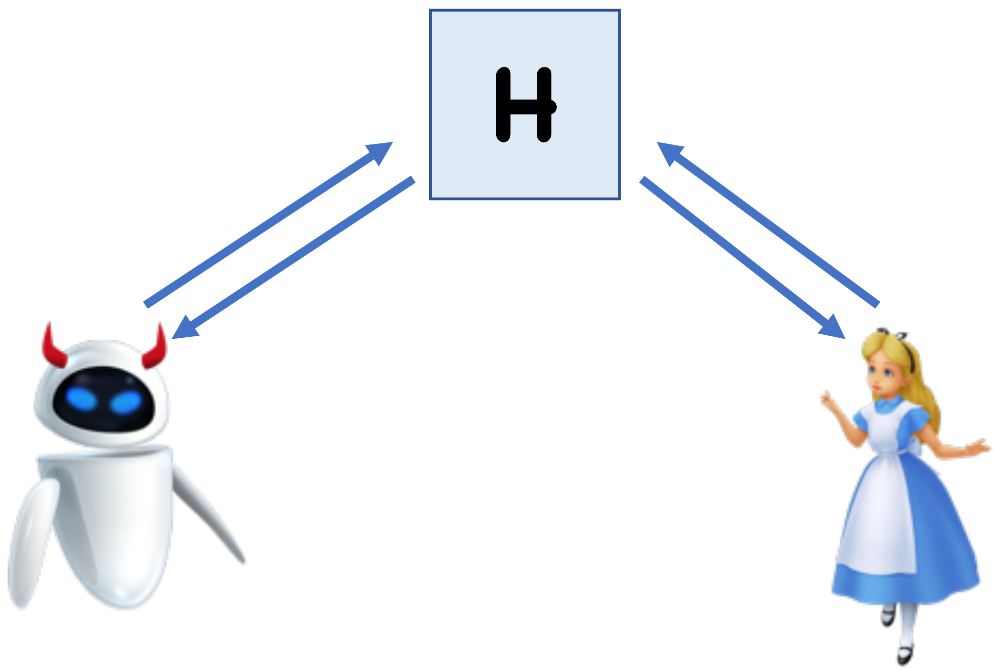
Present a world where one-way functions exist, but collision resistance does not

Hopefully, natural (black box) constructions make sense in this world

- Can construct PRGs, PRFs, PRPs, Auth-Enc, etc

Separating PKE from OWF, CRHF

Recall: random oracle model



Computation power is unlimited, but number of calls to random oracle is polynomial

Separating PKE from OWF

In ROM, despite unlimited computational power, one-way functions, CRHF exist

- $F(x) = H(x)$
- Can only invert oracle by brute-force search (exponentially many queries)
- Can only find collisions by birthday attack (also exponentially many queries)

Separating PKE from OWF

Theorem: If **H** is a random oracle, then for any PKE in which Alice and Bob make at most **n** queries, there is an (inefficient) adversary than makes at most $\mathbf{O(n^2)}$ queries

Intuition: if Alice can send message to Bob, then either
(1) Message can be learned from communication alone, or
(2) Alice and Bob must have a common RO query

In case (2), Alice and Bob's RO queries can't have too much entropy → Adversary can learn with few queries

Cryptocurrency/Blockchain

Features of Physical Cash

Essentially anonymous

Hard to counterfeit

Easy to verify

Limitations of Physical Cash

Cannot be used online

- Instead, need to involve banks
- Banks see all transactions
- Merchants can also track you

Requires central government to issue

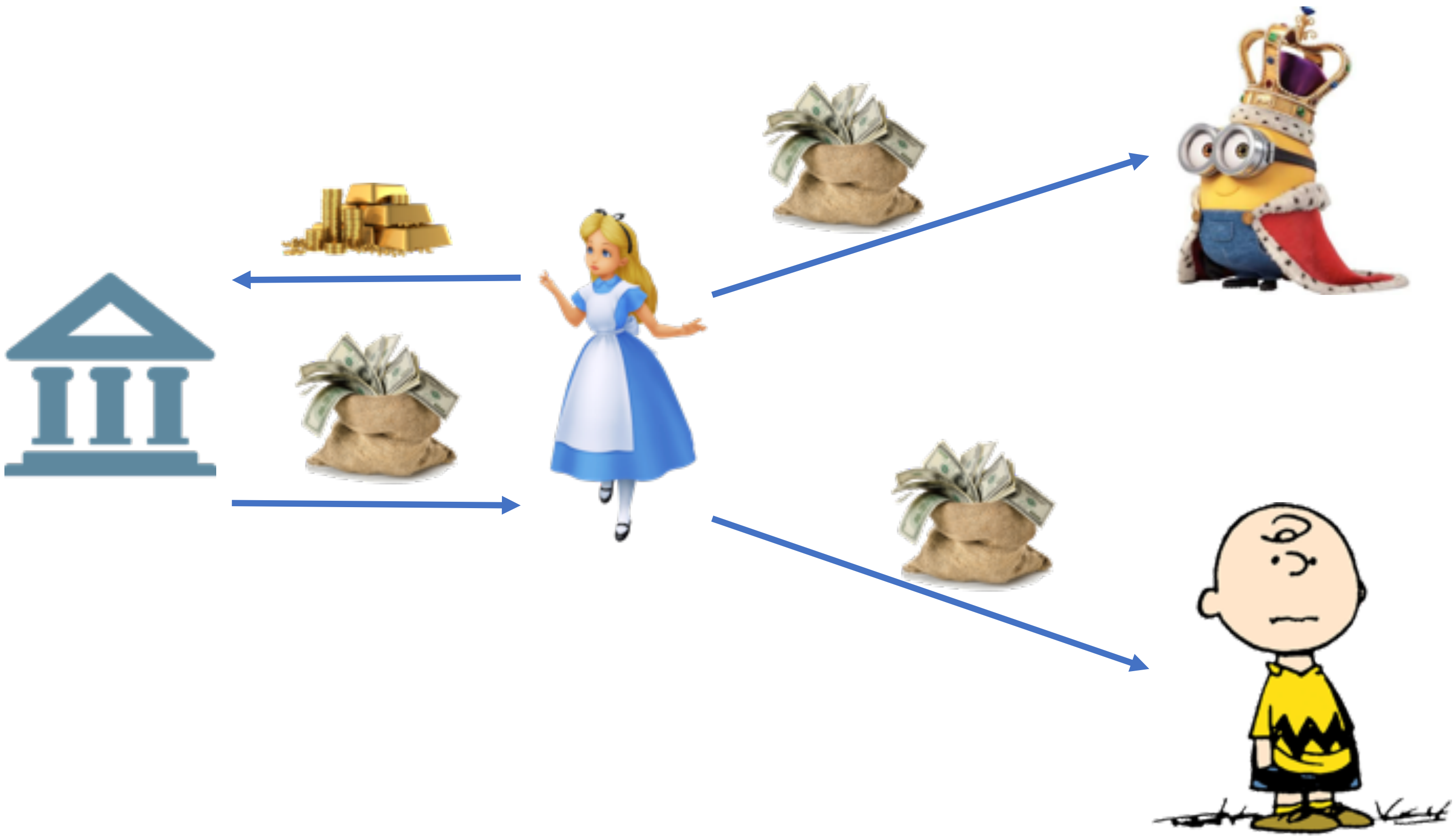
- Ok for most people in US, but maybe you don't trust the government

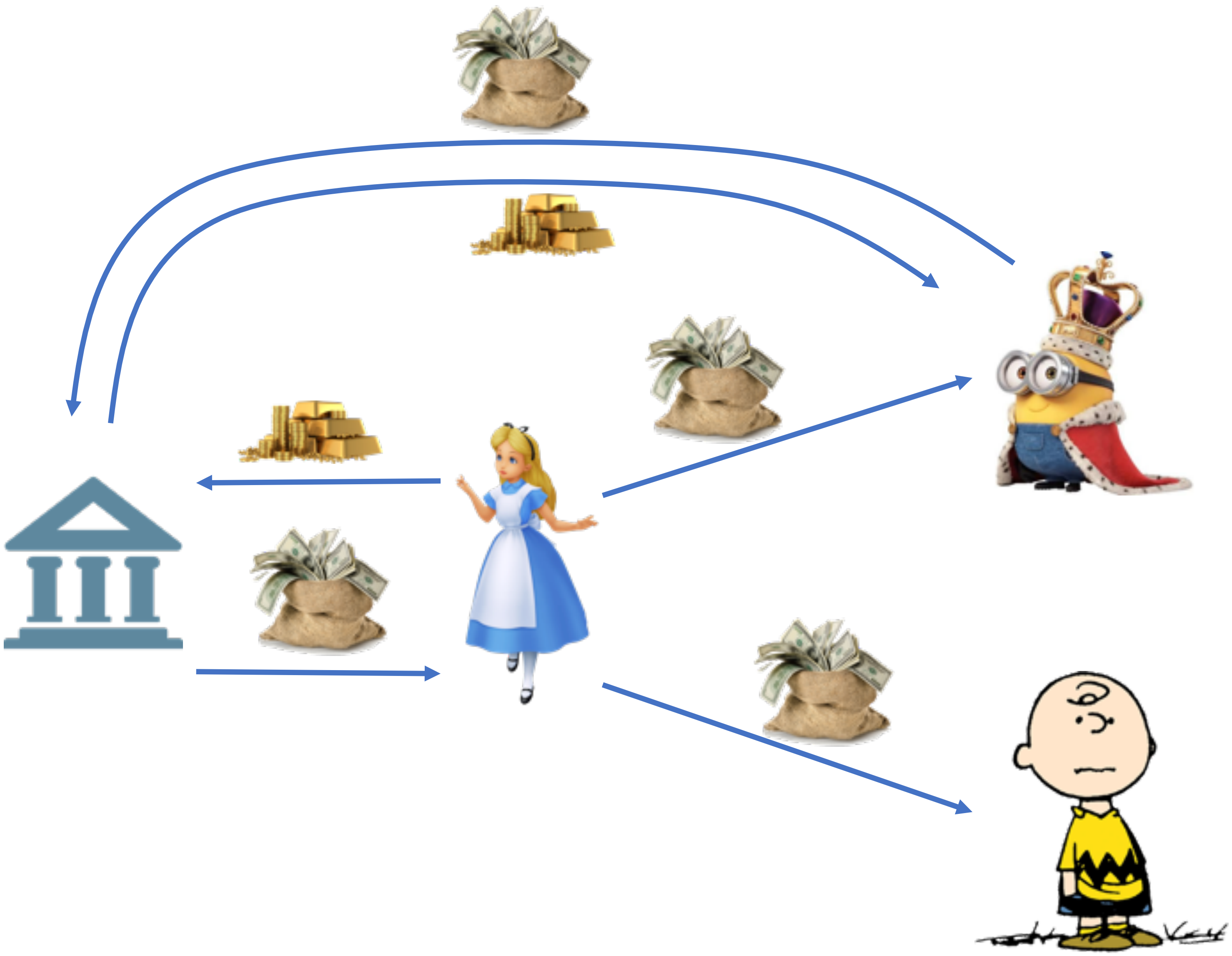
Digital Cash

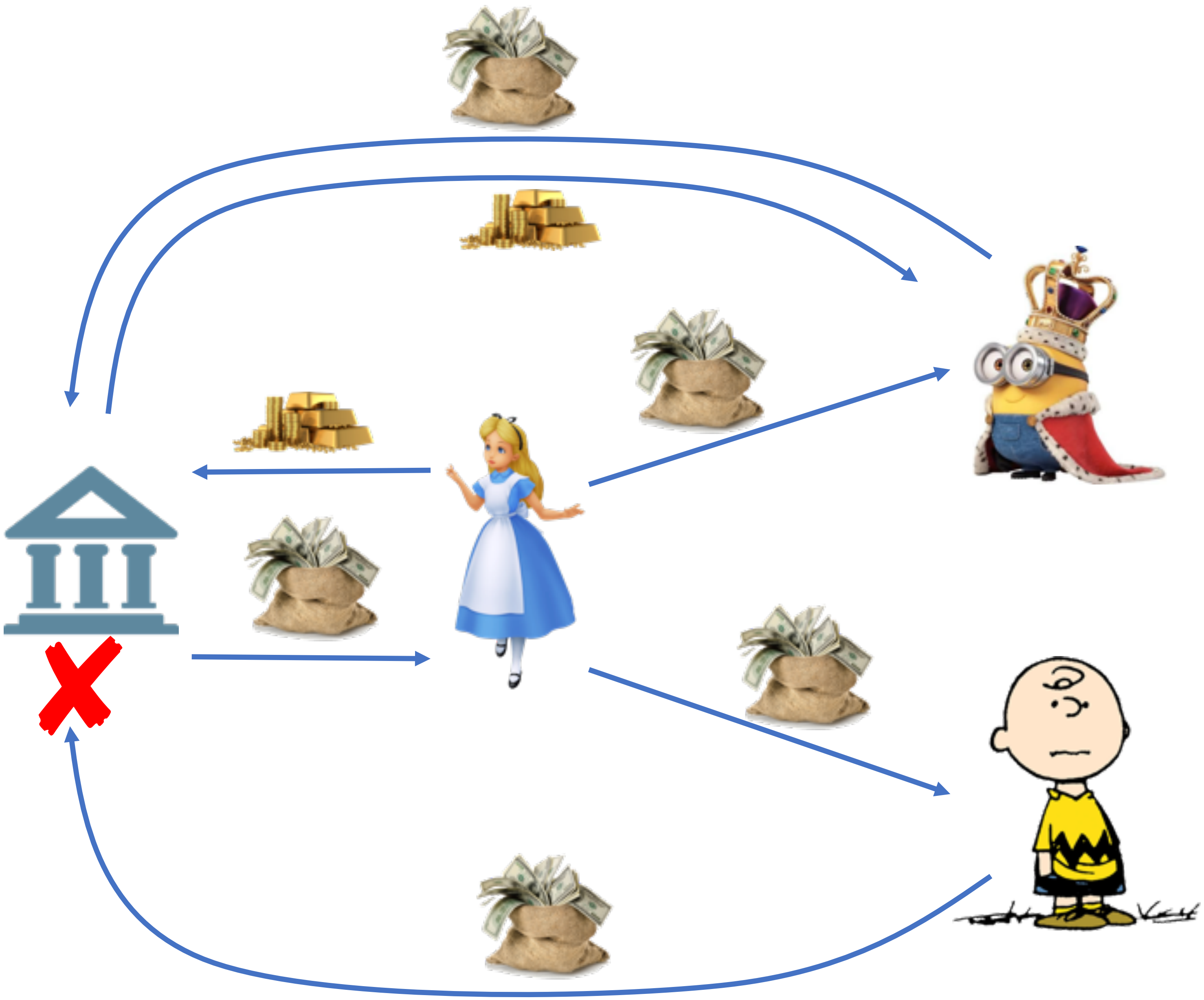
Currency is now 1s and 0s

Crypto can make digital currency easy to verify, hard to mint

Major challenge: prevent double spending
(Also decentralizing minting process)







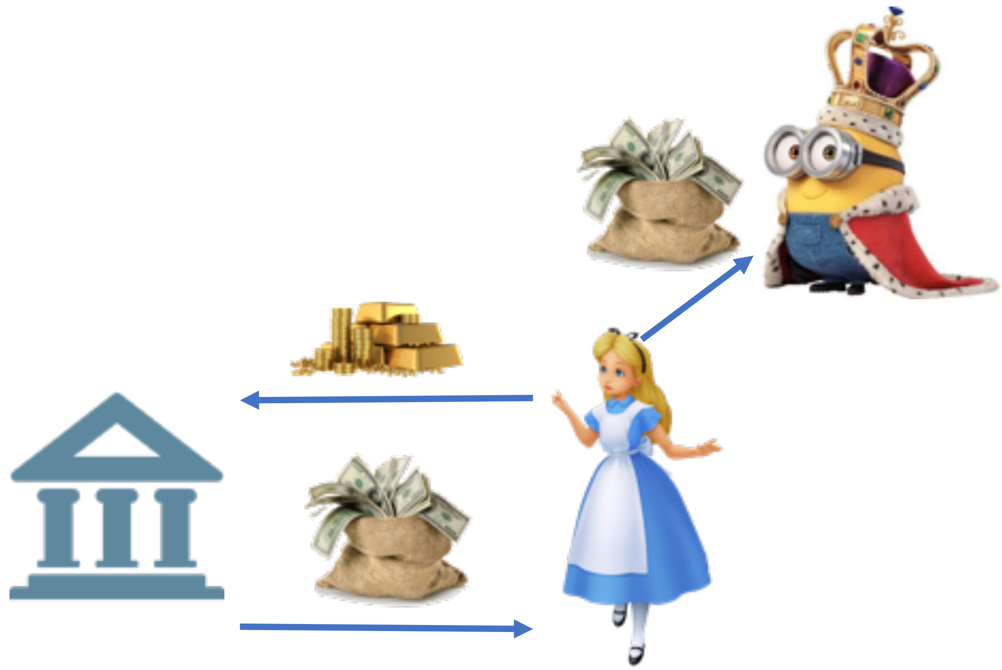
Solution: Public Ledger

Bank transfers $$ to Alice

Each bill has unique serial number

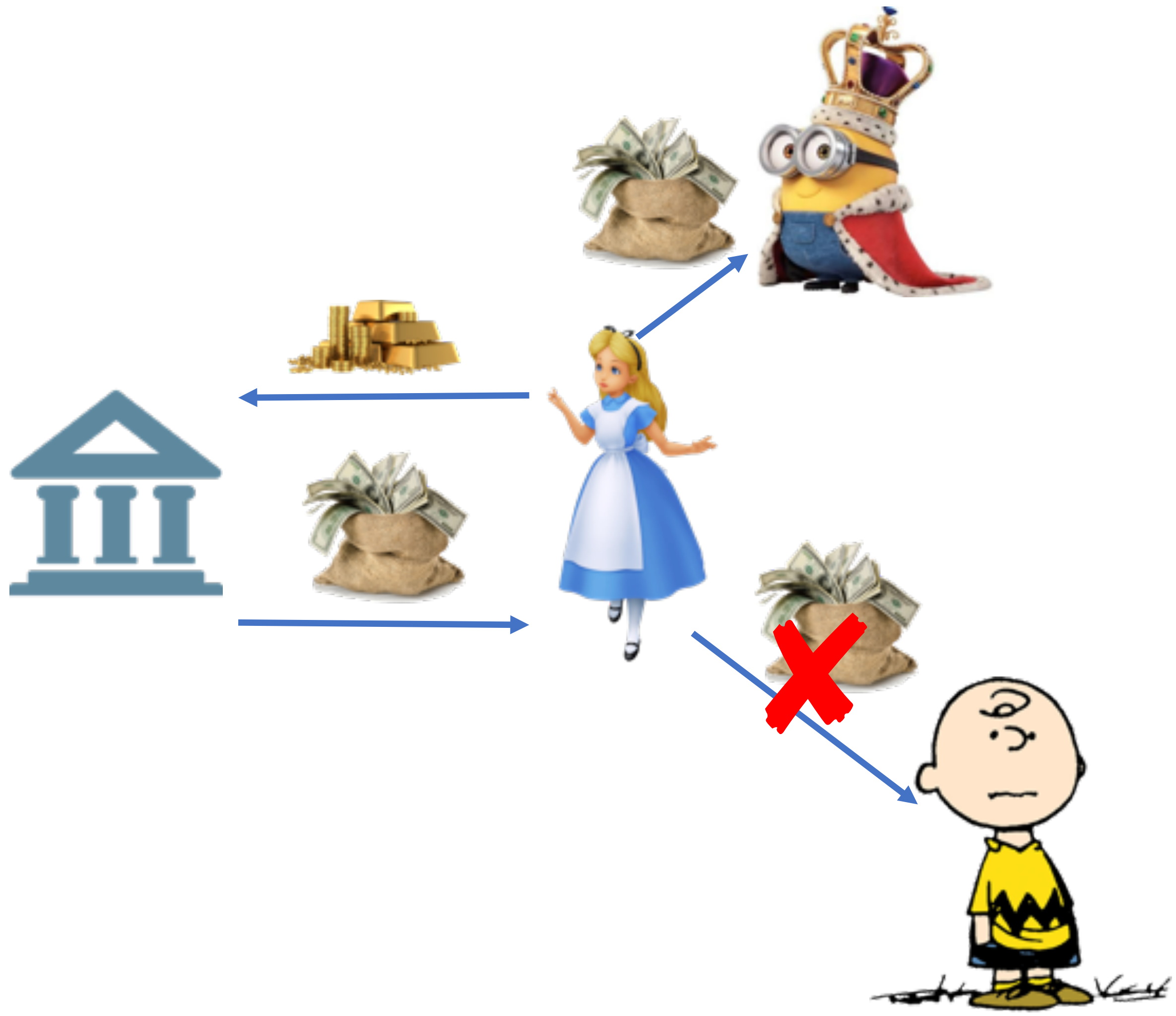
Solution: Public Ledger

Bank transfers $$ to Alice
Alice transfers $$ to Bob



Solution: Public Ledger

Bank transfers $$ to Alice
Alice transfers $$ to Bob



Solution: Public Ledger

Bank maintain ledger?

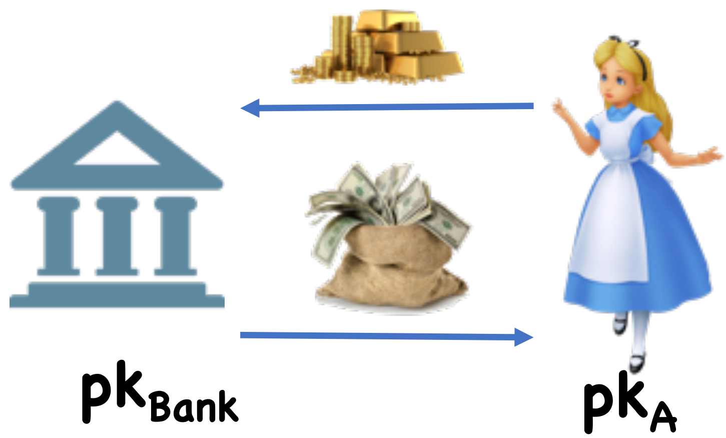
- But then bank must be involved in every transaction
- How does bank prevent malicious Bob from claiming Alice transferred money to him?

Anonymity also lost, since all transactions public

Solution: Use Signatures

pk_{Bank} transfers $$ to **pk_A**, σ_1

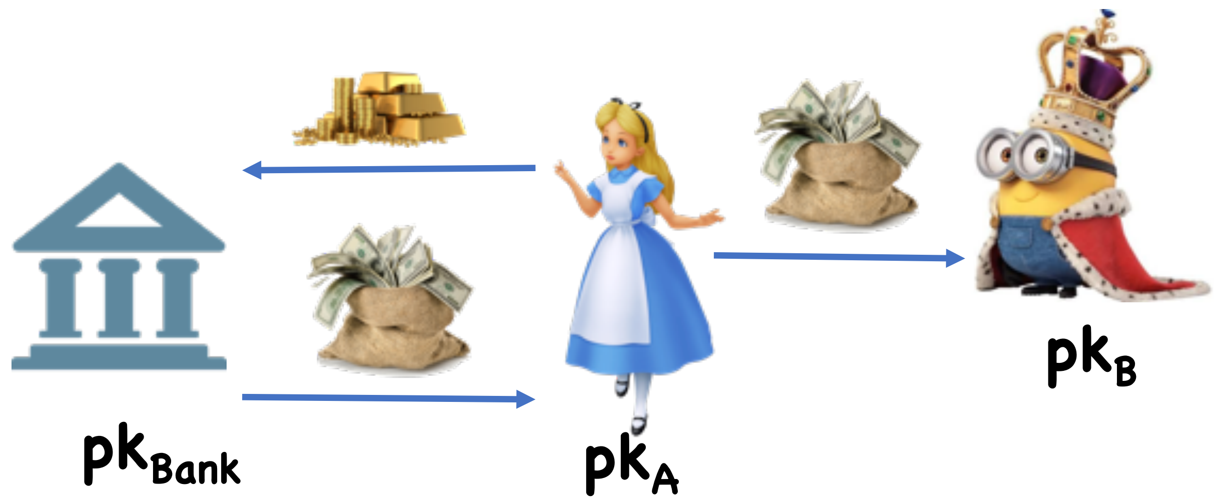
σ_1 = **Sign(sk_{Bank},** "**pk_{Bank}** transfers $$ to **pk_A**")



Solution: Use Signatures

$\mathbf{pk_{Bank}}$ transfers \$\$ to $\mathbf{pk_A}$, σ_1
$\mathbf{pk_A}$ transfers \$\$ to $\mathbf{pk_B}$, σ_2

σ_2 = **Sign(**$\mathbf{sk_A}$, "$\mathbf{pk_A}$ transfers \$\$ to $\mathbf{pk_B}$")



Solution: Use Signatures

By using public key as identity, transactions not immediately traced to individual

- Though can still trace sequences of transactions

By signing, prevents Bob from claiming Alice gave him money when she didn't

Decentralized Currency

Removing the bank is hard:

- How is ledger maintained?
- How to prevent ledger from being tampered with
- Who mints new currency?
- How do we limit supply?

Proofs of Work

Prove that some amount of computation has been performed

Ex:

- Let **H** be a hash function (modeled as a RO)
- An input **x** such that $\mathbf{H(x) = 0^{t}*****}$ is a "proof" that you computed approximately $\mathbf{2^{t}}$ hashes

Proofs of Work and Cryptocurrency

Idea: currency is a proof of work

- Limits supply of money, so keeps inflation in check
- Now, anyone can mint new money

Proofs of work not the only option

- Proofs of stake
- Proofs of space

Blockchain

Immutable public ledger

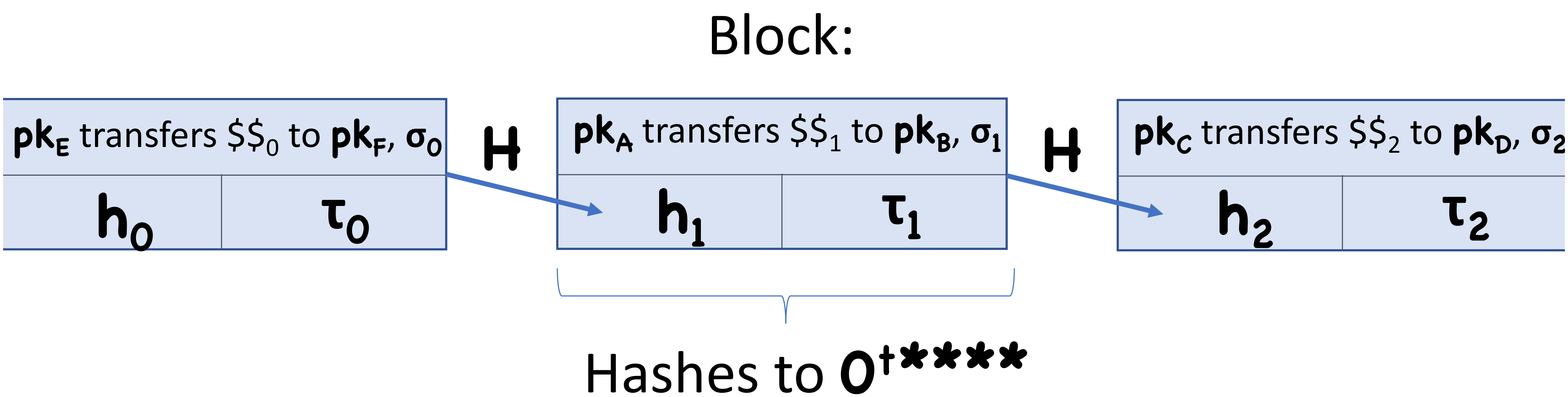
Block:

pk_A transfers $\$\$_1$ to pk_B, σ_1	
h_1	τ_1

Hashes to 0^t****

Blockchain

Immutable public ledger



Blockchain

By making each block a proof of work, hard to modify blockchain

So proofs of work used to:

- Mint new money
- Add transactions to blockchain

Why would anyone go through the effort of adding transactions to the blockchain?

Blockchain

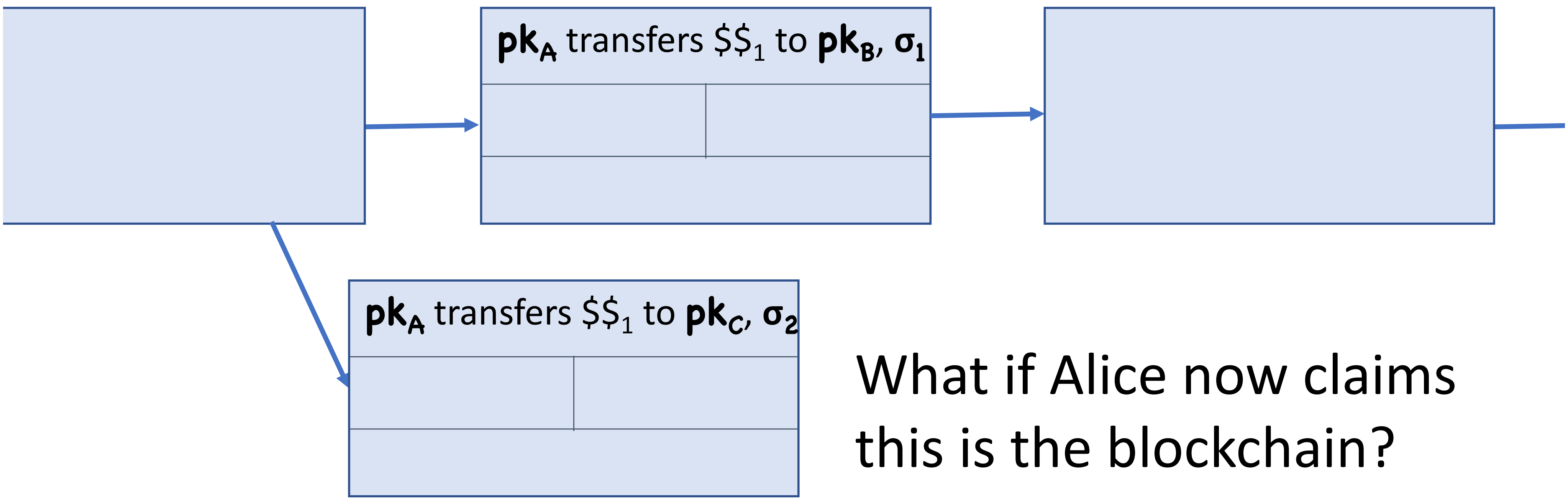
Idea: combine minting and adding blocks

Block:

$\mathbf{pk_A}$ transfers $\$\$_1$ to $\mathbf{pk_B}$, σ_1	
h_1	τ_1
$\mathbf{pk_M}$ mined $\$\$_M$	

Hashes to $0^t{*}{*}{*}{*}$

Double Spending



What if Alice now claims this is the blockchain?

Double Spending

To prevent double spending, everyone always uses longest chain as the blockchain

If Alice tries to double spend, she will need to create a separate chain that is as long as the main chain

- As long as she has <<50% of computing power of mining power, will not be possible