

The Jekyll and Hyde of Smart Contracts

Ari Juels

Jacobs Institute, Cornell Tech
Co-Director, IC3

Guest lecture, CS 5112
20 Sept. 2018



INSIDE: A 12-PAGE SPECIAL REPORT ON COLOMBIA

Our guide to America's best colleges
Myanmar's free-ish election
Those ever-creative accountants
America takes the fight to IS
Coywolves: the new superpredator

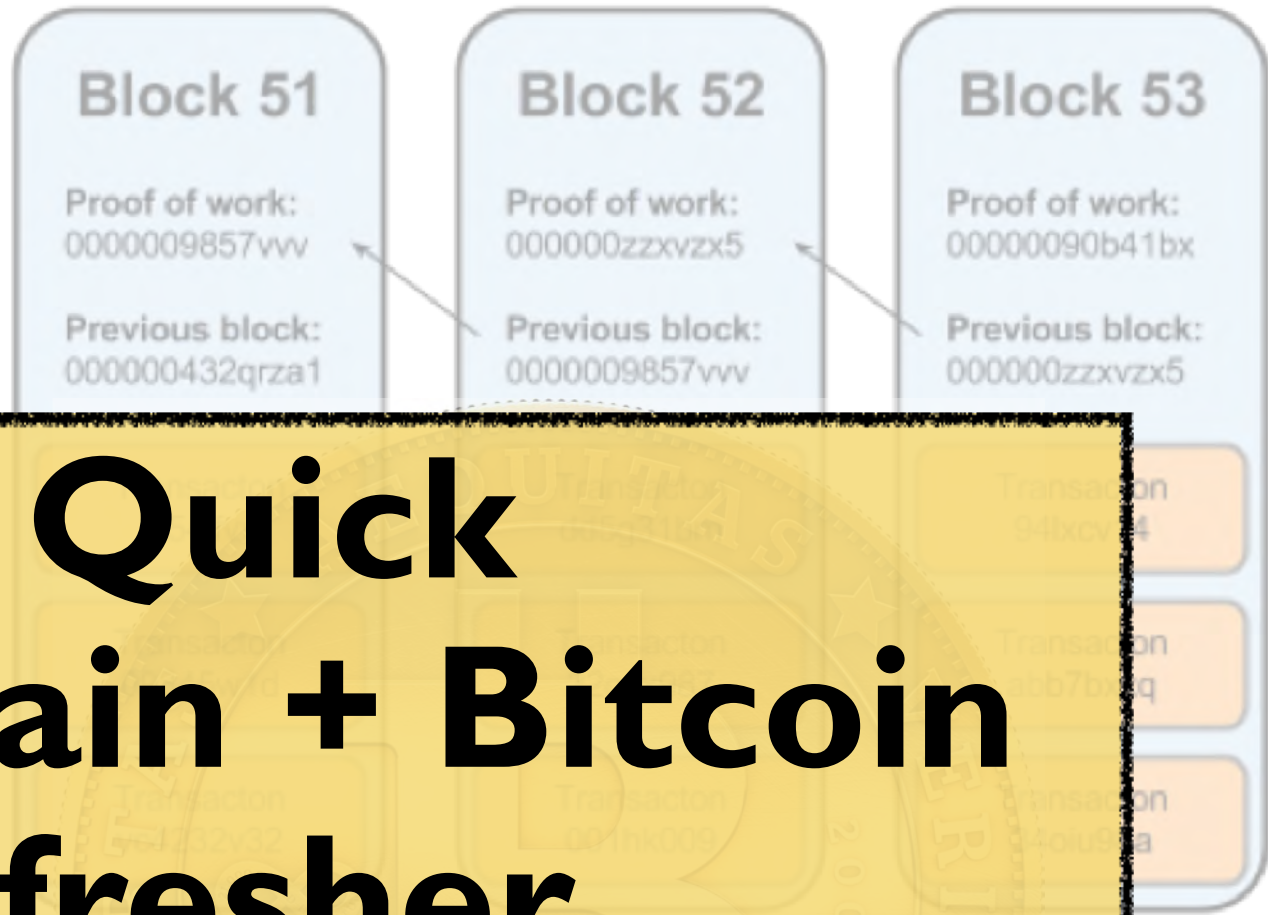
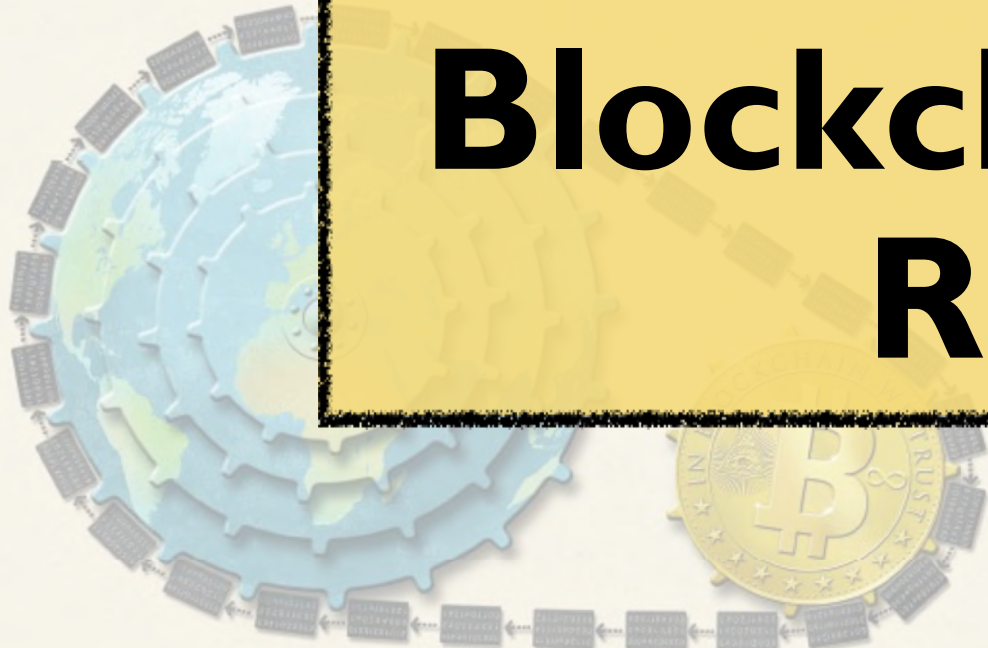
The Economist

OCTOBER 31ST-NOVEMBER 6TH 2015

Economist.com

The trust machine

How the technology behind bitcoin could change the world



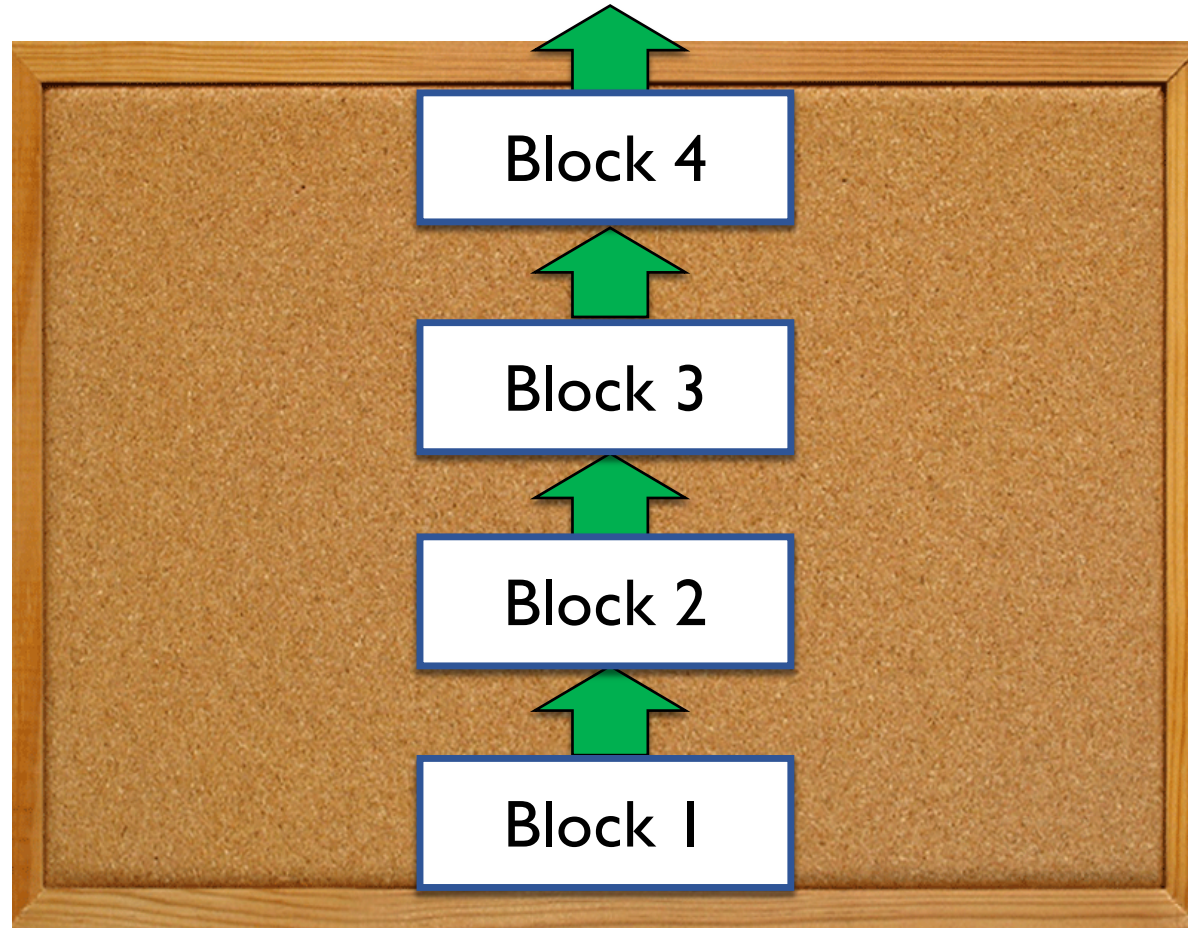
A Quick Blockchain + Bitcoin Refresher



Australia.....AU\$12.00	China.....¥18.00	France.....€12.00	Germany.....€12.00	India.....₹180.00	Japan.....¥1,800.00	South Korea.....₩18,000.00	Switzerland.....CHF 12.00	Taiwan.....NT\$200.00	USA.....\$12.00
Canada.....C\$18.00	Italy.....€12.00	Malaysia.....RM48.00	Spain.....€12.00	UK.....£12.00	USA.....\$12.00	USA.....\$12.00	USA.....\$12.00	USA.....\$12.00	USA.....\$12.00

Blockchains: Abstraction

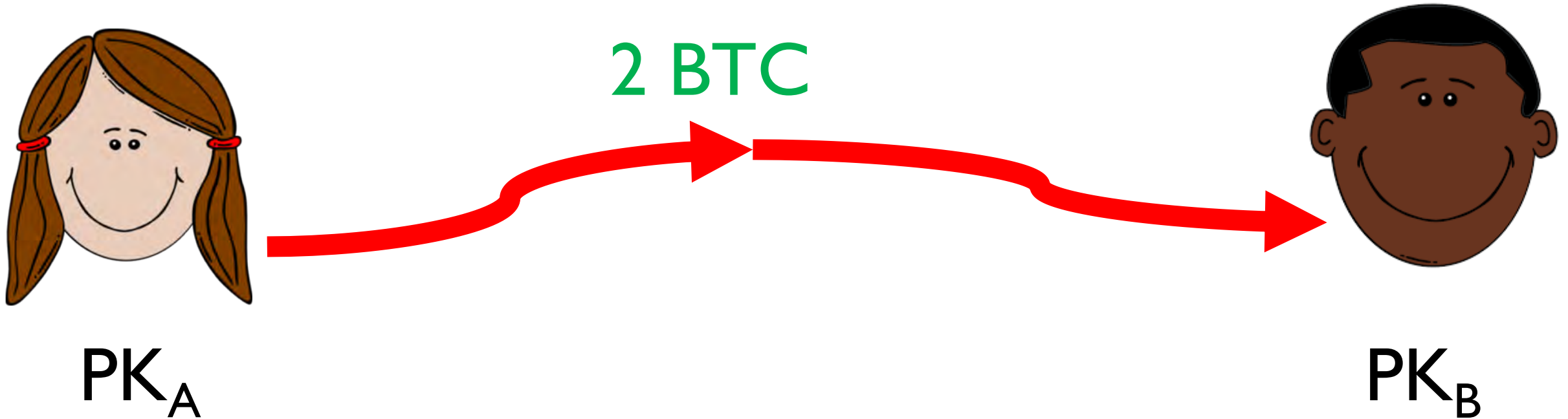
Write
Permission:
Any valid data



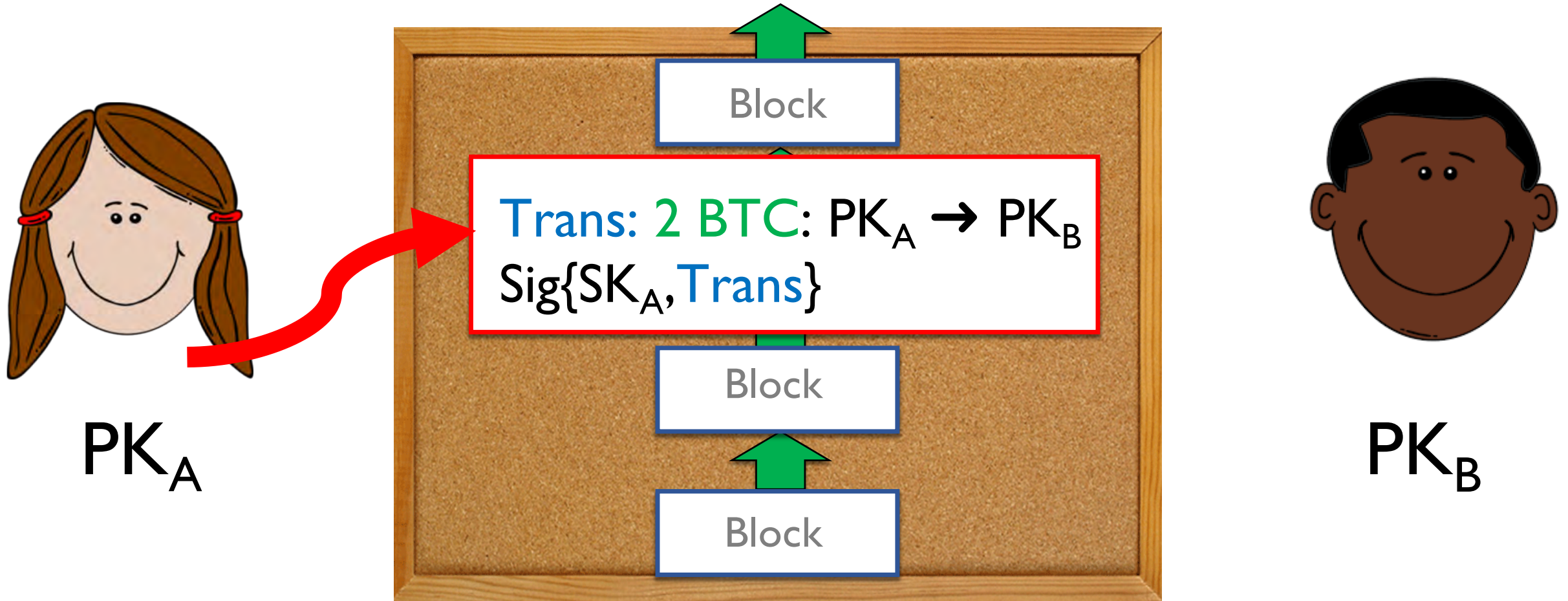
Read
Permission:



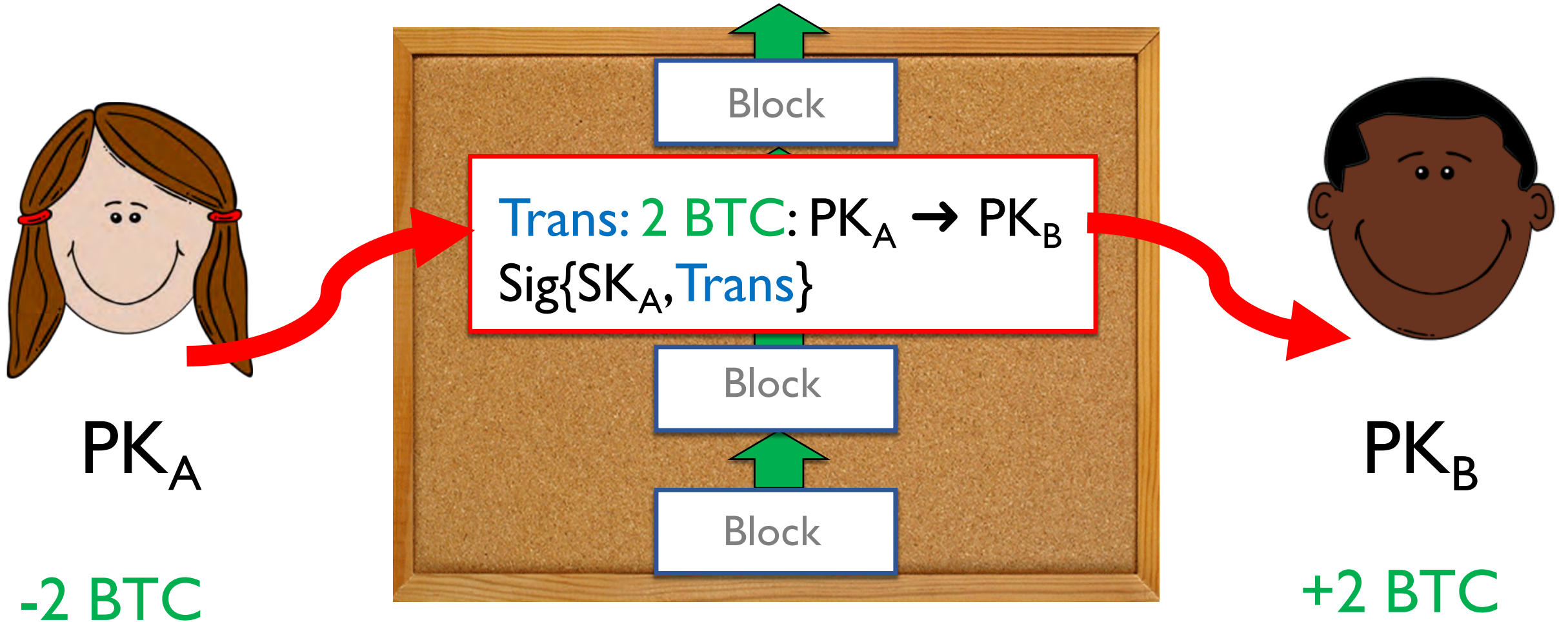
Bitcoin's use of a blockchain



Bitcoin's use of a blockchain



Blockchain = Trusted (universal) memory



Simple abstraction → Powerful benefits

- Bitcoin offers:
 - Anonymous (pseudonymous) transactions
 - Unstoppable payments
 - Irrevocable
 - No interference by authorities

Bitcoin has many good uses!

- Low transaction fees + no middlemen
 - Low-cost payments
- Key-based bearer instrument
 - High portability
- Decentralized
 - Fast cross-border remittances

But... anonymity +
unstoppable payments =

**Excellent tool for
crime!**



Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue

Ransomware!

1989 PC Cyborg Trojan

Your personal files are encrypted



Your files will be lost
without payment on:

11/24/2013 3:16:34 PM

Info

Your **important files were encrypted** on this computer: photos, videos, documents, etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key **RSA-4096** generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

See files

<< Back

Proceed to payment >>

Other Bitcoin-fueled mischief

The screenshot shows the Silk Road anonymous marketplace website. The browser window title is "Welcome! | Silk Road" and the address bar shows "silkroadvb5piz3r.onion". The website header includes the Silk Road logo (a green camel) and the text "Silk Road anonymous marketplace". User information shows "Welcome Cult Leader!" with links for "messages(0)", "orders(0)", "account(\$0.00)", "settings", and "log out". A search bar and a shopping cart icon with "(0)" are also visible.

8 days 2 hrs 51 mins 31 secs until **Four Twenty!!!**

Shop by category:

- Drugs(2679)
 - Cannabis(741)
 - Dissociatives(59)
 - Ecstasy(274)
 - Opioids(214)
 - Other(76)
 - Prescription(515)
 - Psychedelics(348)
 - Stimulants(256)
- Apparel(22)
- Books(283)
- Computer equipment(13)
- Digital goods(220)
- Drug paraphernalia(52)
- Electronics(19)
- Fireworks(1)
- Forgeries(41)
- Hardware(3)
- Home & Garden(5)
- Jewelry(1)

News:

- Who's your **favorite?**
- Acknowledging **Heroes**
- A new anonymous market **The Armory!**
- **State of the Road Address**

 <p>CRANBERRY KUSH & STRAWBERRY... \$36.82</p>	 <p>10pc of Genuine Fake Blu Ray Discs \$49.50</p>	 <p>30mg Oxycodone (Roxie, Roxo) IR... \$250.00</p>
 <p>BITCOINS - NOW THE LOWEST PRICE... \$0.00</p>	 <p>Diazepam (valium) 10mg - 1000... \$425.50</p>	 <p>Anarcho47's Magikally Epic... \$2.48</p>
		

A black electric guitar is shown from a front-three-quarter view, completely surrounded by intense, bright orange and yellow flames. The guitar's body is black, and its pickguard is white with two humbucker pickups, a bridge, and a control plate with knobs and a pickup selector. The neck is dark with white frets and a headstock. The background is dark, making the fire and the guitar stand out. A semi-transparent yellow rectangular box is centered over the guitar, containing bold black text.

**Decentralized smart
contracts will *amp it all up***

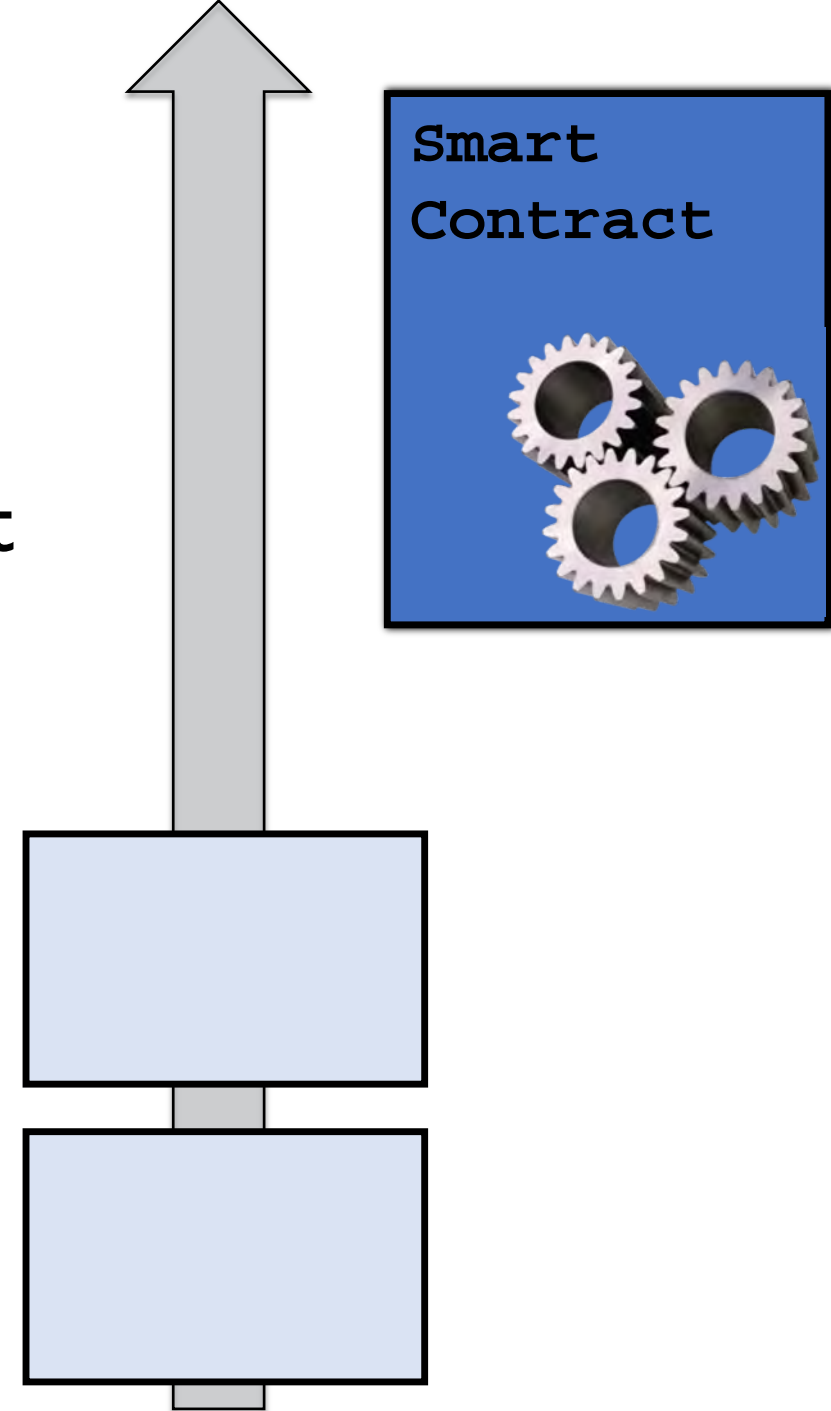


What's a Smart Contract?

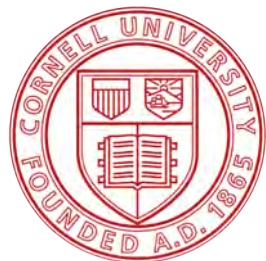
- Type interpreted by operations
- Only stack & alt-stack
- No return stack (no calls)
- No heap
- Deterministic - No side effects or I/O

Smart contracts

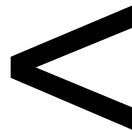
- Small programs that run on *blockchains*
- Given trust in underlying blockchain, smart contracts are
 - Transparent
 - Irreversible
 - Tamper-resistant
- ...plus they can act upon **crypto tokens = \$money**



Lots of recent interest in ETH...

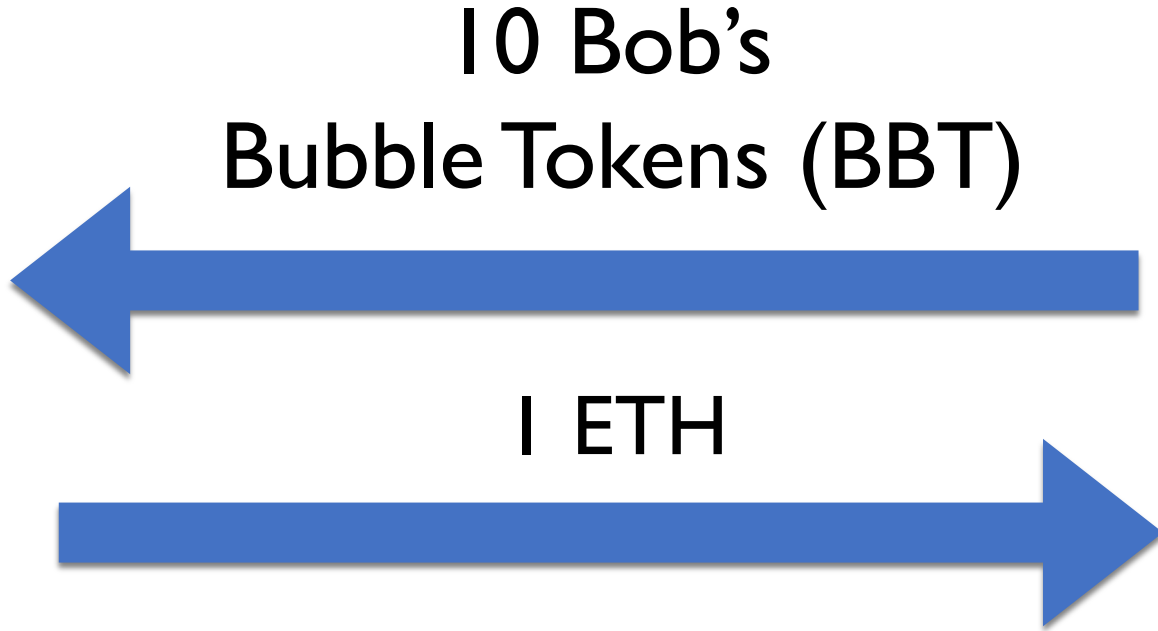
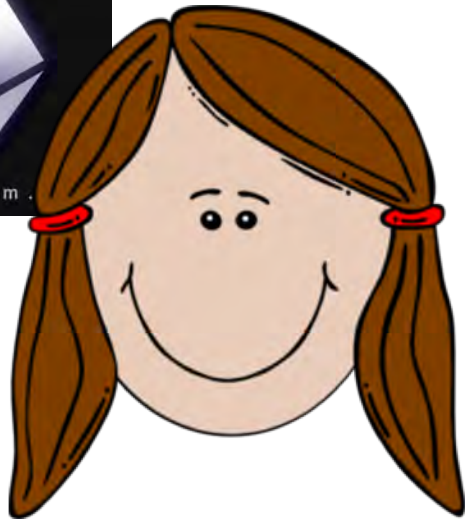


\$7 billion



> \$20 billion

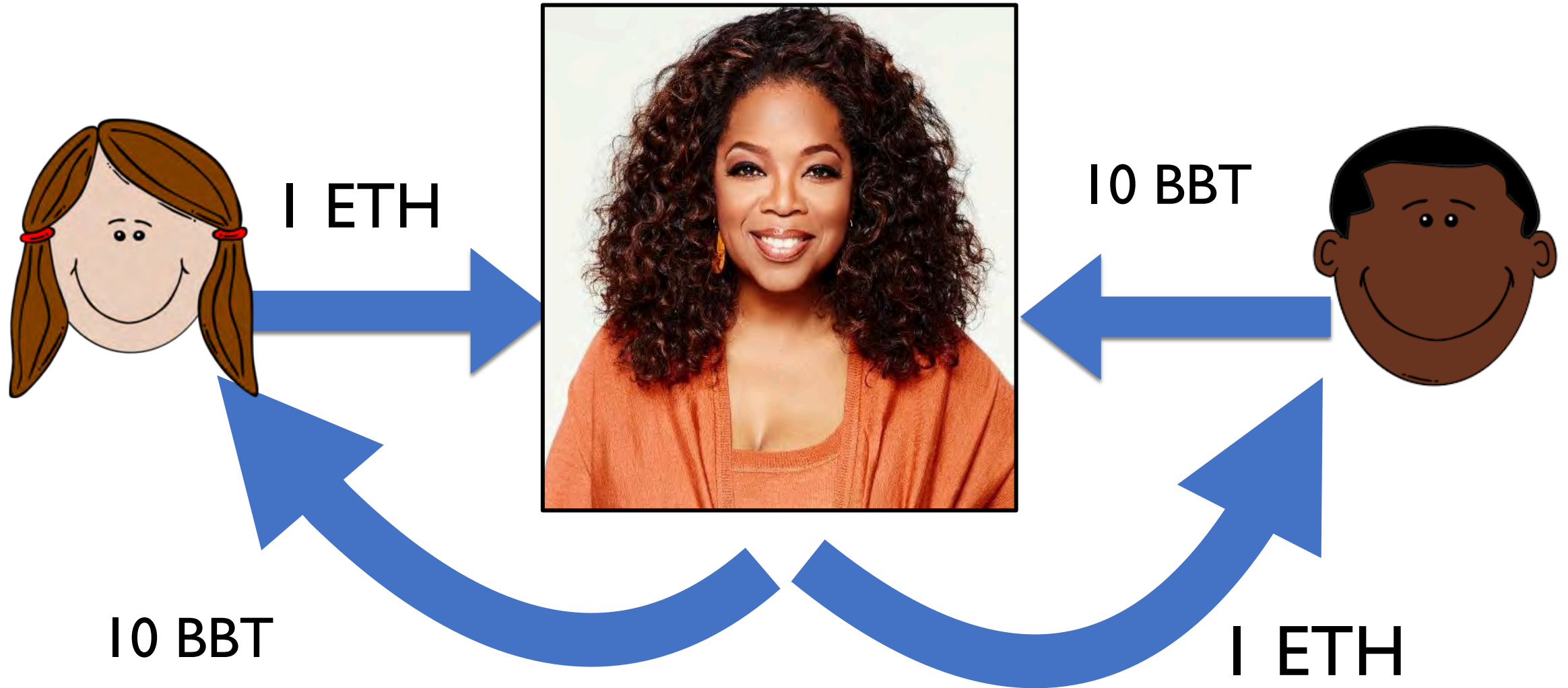
Why? Suppose Alice and Bob want to trade..



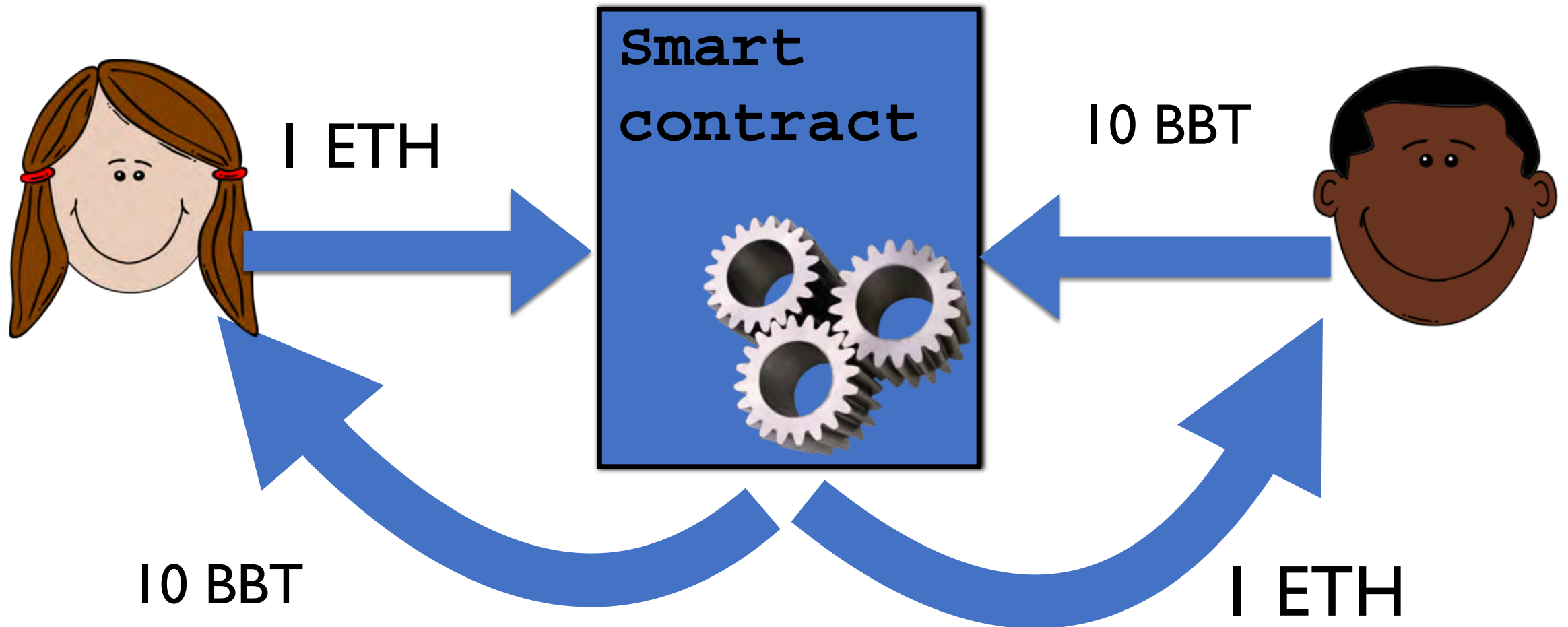
Bob's Bubble Tokens (BBT)

Problem of *Fair Exchange!*

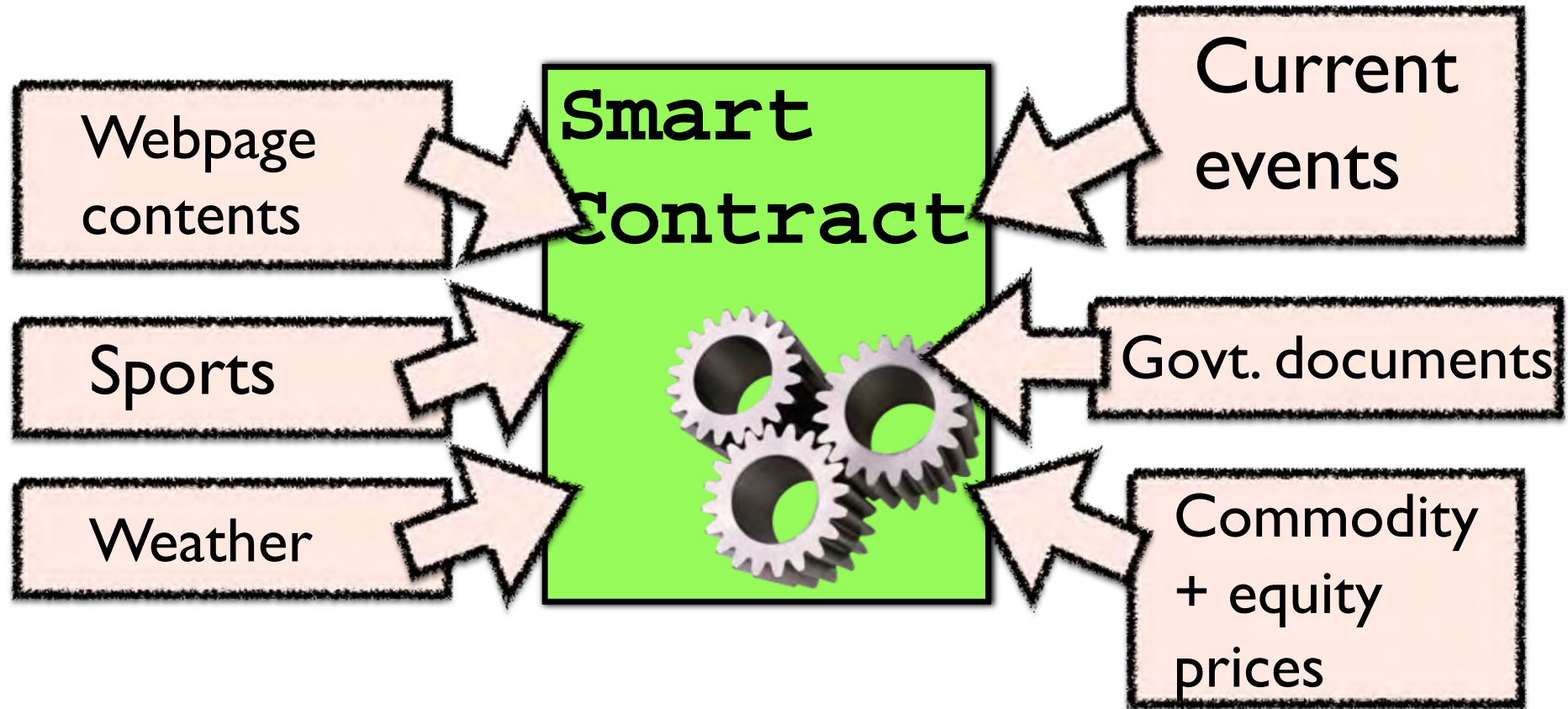
Trusted third-party (with public state)



Smart contract \approx Trusted third-party (with public state)



Plus, they'll have oracles...





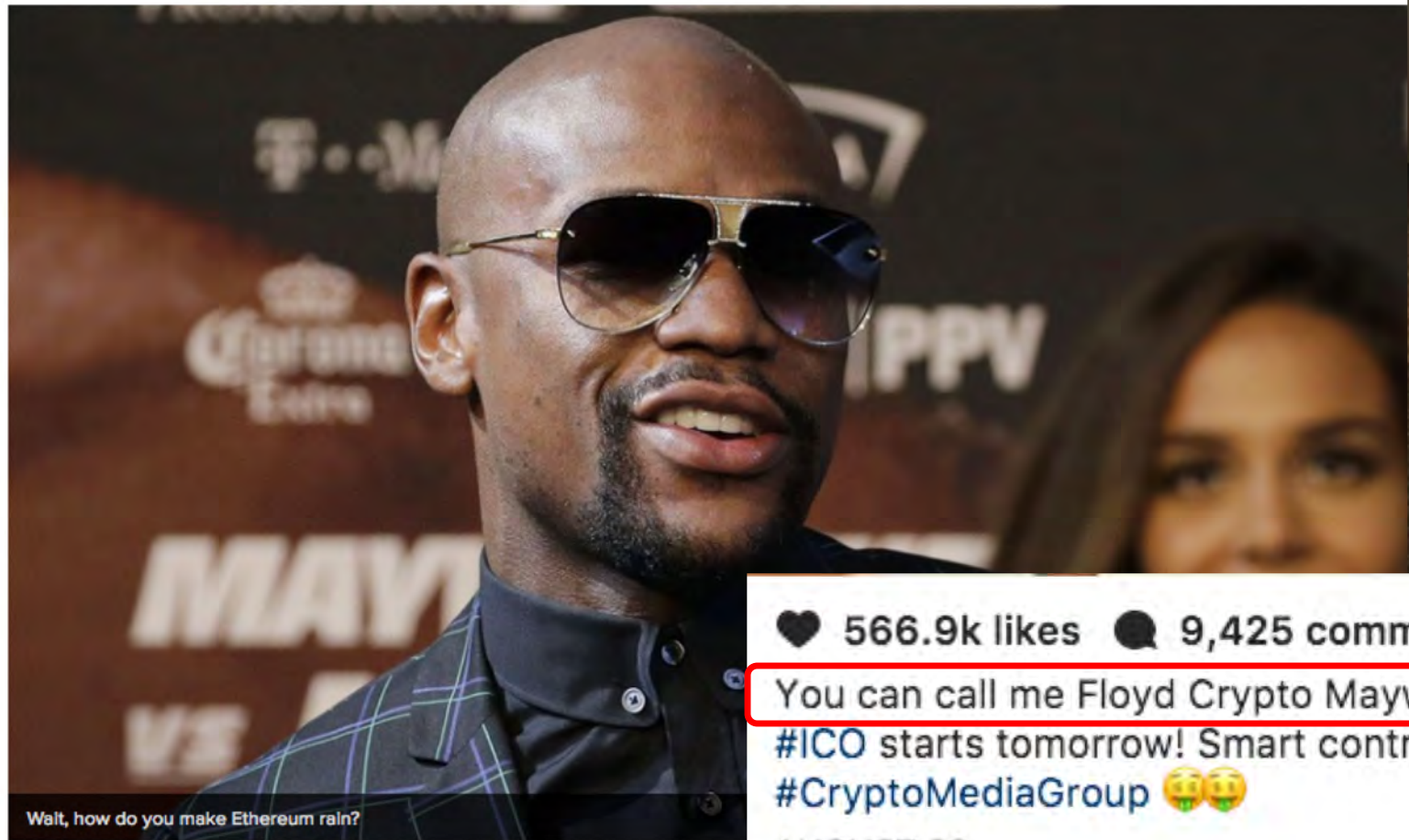
No, not
Floyd Mayweather...

Floyd 'Crypto' Mayweather promotes an ICO, again



Mashable

AUG 24, 2017



❤️ 566.9k likes 💬 9,425 comments

You can call me Floyd Crypto Mayweather from now on...Hubii.Network
#ICO starts tomorrow! Smart contracts for sports?! #HubiiNetwork
#CryptoMediaGroup 🍀🍀

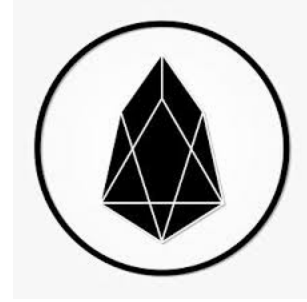
AUGUST 23

Wait, how do you make Ethereum rain?



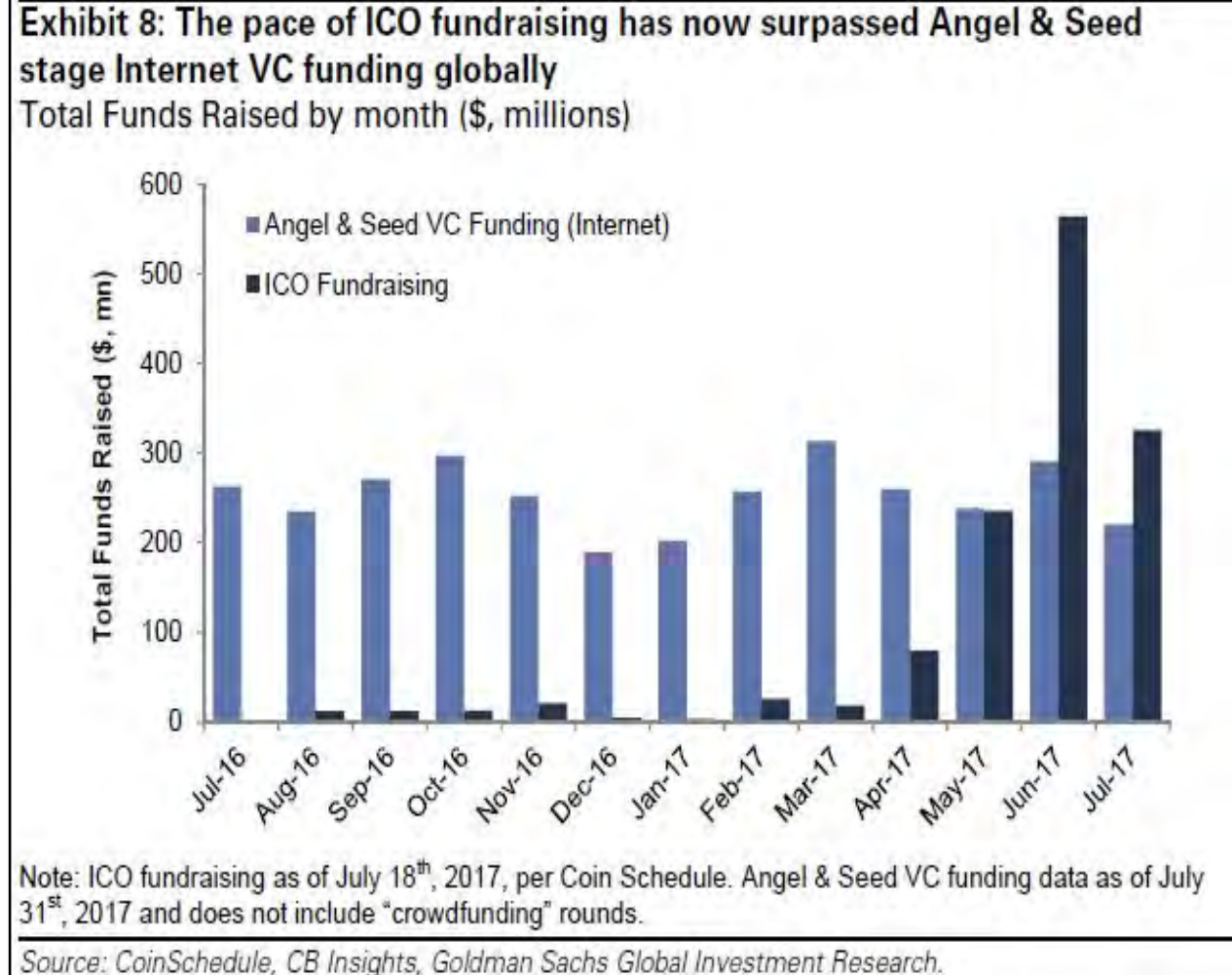
Crypto Tokens

- Application-specific cryptocurrency
- Mainly ERC20 tokens
 - Managed in Ethereum smart contracts
- \$13+ billion token market cap



Crypto Tokens

- Sold in Initial Coin Offerings (ICOs)
 - a.k.a. Token Launch, Token Generation Events (TGEs), etc.
 - Like unregulated VC
 - Token like a share (kind of...)
- Since mid-2017, ICO funding outstripping early-stage Internet VC (!)

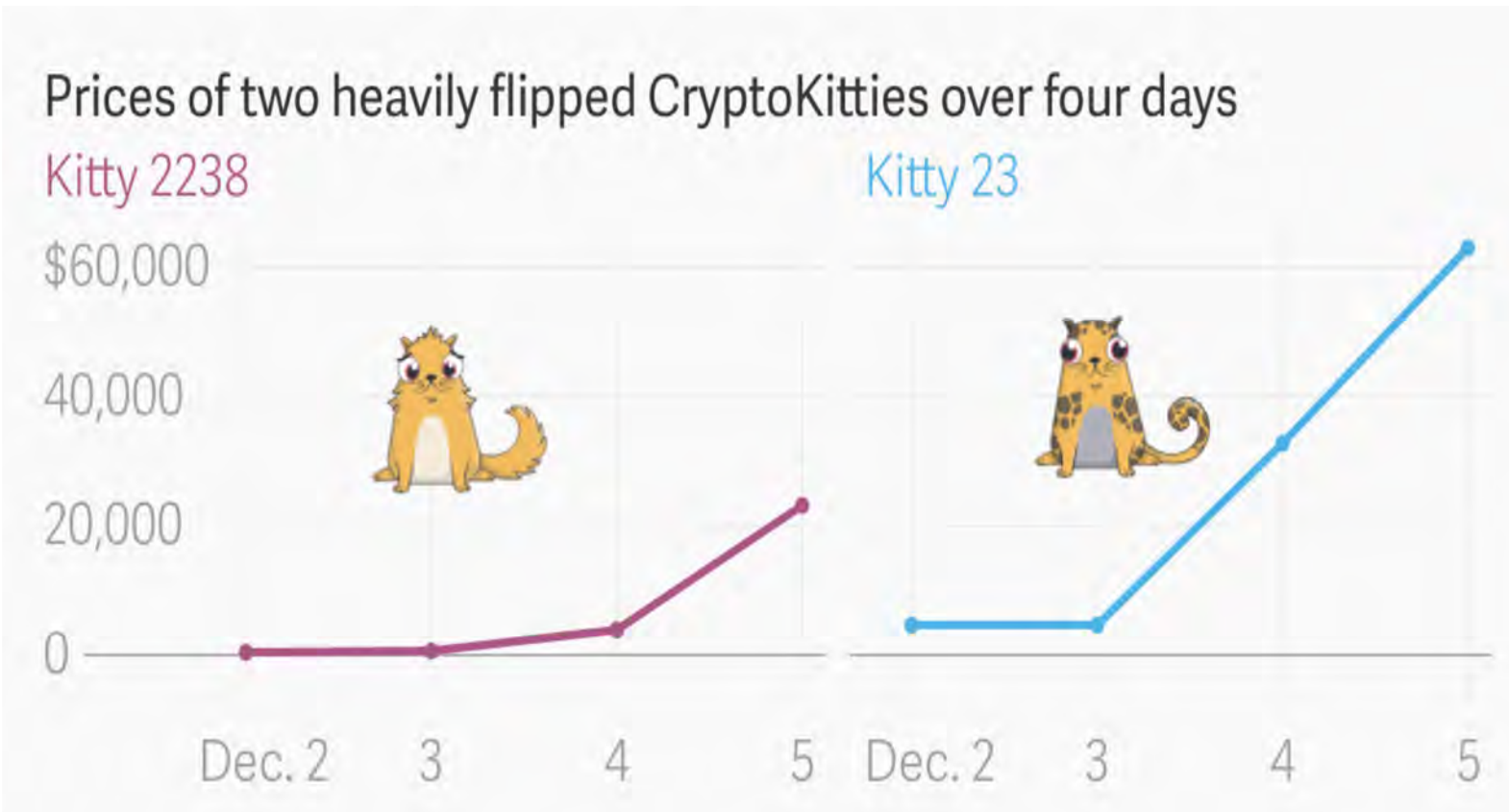


Crypto Tokens: ERC721

- “Non-fungible tokens”: Represent unique objects



CryptoKitties



Simple smart contract: Lottery

Contract Lottery

Lottery



Simple smart contract: Lottery

Contract Lottery

Init:

```
Tend := 30 Sept 2016,  
$ticket := 1,  
pool := {},  
pot := 0
```

TicketPurchase:

```
On receive $amt from party P:  
  Assert $amt = $ticket, balance[P] ≥ $amt  
  balance[P] := balance[P] - $ticket  
  pot := pot + $ticket  
  pool := pool ∪ P
```

Timer:

```
If T > Tend then  
  W ∈R pool  
  balance[W] := balance[W] + pot
```



Lottery

Criminal Smart Contracts



Ari Juels, Ahmed E. Kosba, Elaine Shi: The Ring of Gyges: Investigating the Future of Criminal Smart Contracts. ACM CCS 2016.

The F3 For Security Hacked !!!!!

Criminal Smart Contracts (CSCs)

- Smart contracts address inefficiencies in business transactions.
 - E.g., make raising venture capital more efficient via tokens
- CSCs address inefficiencies in criminal business transactions.
- CSCs reap anonymity and distributed trust to:
 - Solicit perpetration of crimes or
 - Sell criminal services.

CSCs solve two major (criminal) business problems

I. Dangerous trust model / reliance on reputation!

- Cybercrime supersite DarkMarket.ws
 - Site admin Master Splyntr = FBI agent K. Mularski!
- Ross Ulbricht (DPR, Silk Road) solicited six murders for hire
 - ...including one from the FBI
 - FBI staged torture and murder to entrap Ulbricht



CSCs solve two major (criminal) business problems



2. Law enforcement can shut you down.

CSCs solve both problems by enforcing trust

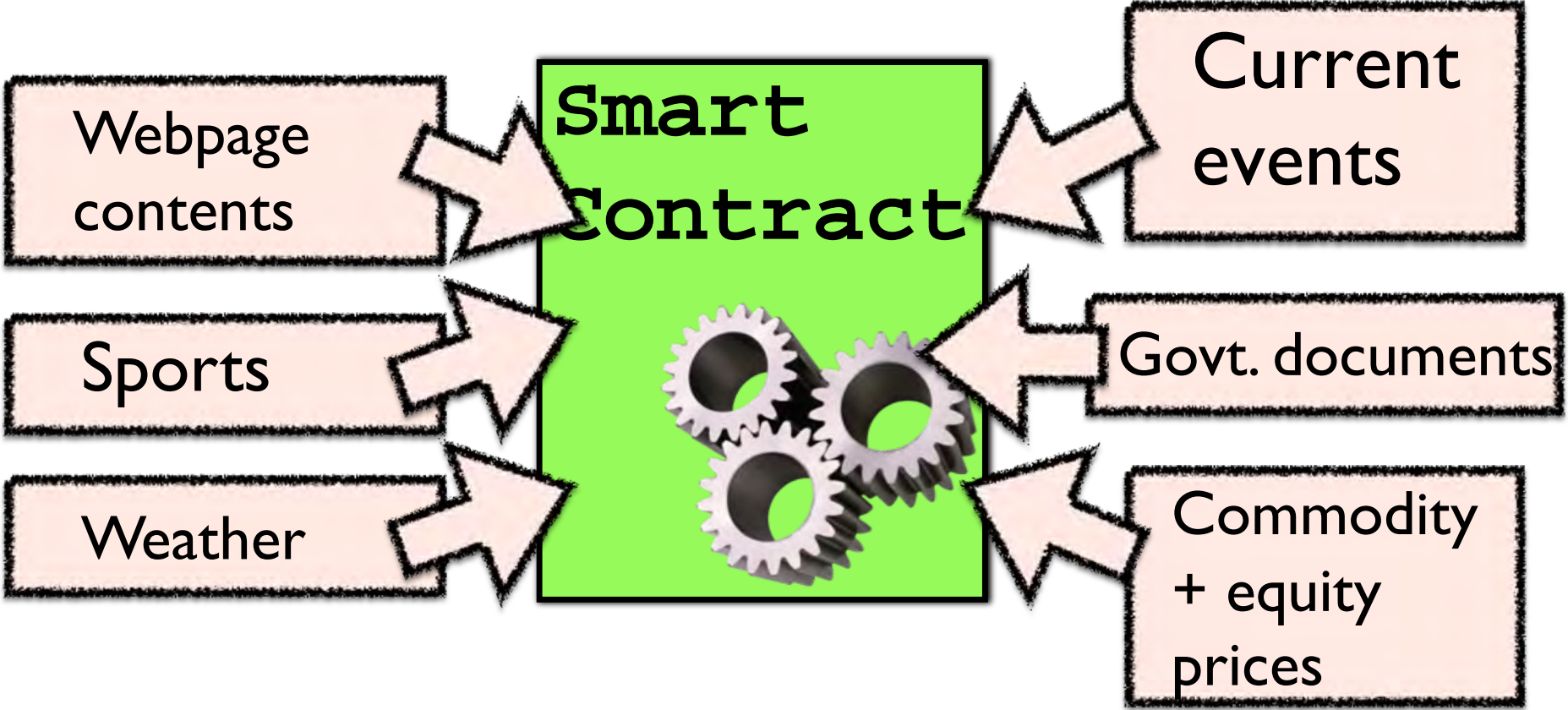
- Main mechanisms: *anonymity* and *autonomous execution*
- CSCs can achieve ***commission fairness***
- **Commission fairness:** *both* commission of a crime and commensurate payment for perpetrator or *neither*

Contract: Assassination

- C offers \$reward (e.g., \$1,000,000) for assassination of CEO X
- How to verify:
 1. That assassination happened?
 2. That a claimed perpetrator \mathcal{P} was actually responsible?
- Solutions:
 1. **Authenticated data feed / oracle**



Assume...



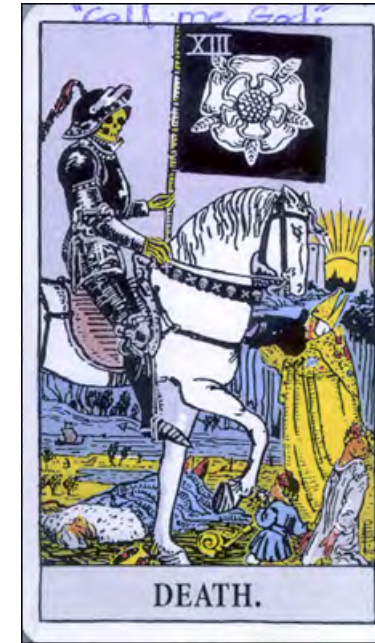
Contract: Assassination

- C offers \$reward (e.g., \$1,000,000) for assassination of CEO X
- How to verify:
 1. That assassination happened?
 2. That a claimed perpetrator \mathcal{P} was actually responsible?
- Solutions:
 1. Authenticated data feed / oracle
 2. **Calling card**



Calling card

- Traditionally, exotic object left by a criminal
 - E.g., Beltway Sniper's tarot cards (2002)
- For CSC, calling card **CC** is set of details of crime that are:
 1. Hard to guess in advance; and
 2. Reported (by media) in authenticated data feed.
- Example details:
 - Day, time, place
 - Unusual keywords captured in news
 - E.g., Litvinenko poisoned with "Polonium-210" (2006)



Beltway Sniper



"The Phantom"

How does \mathcal{P} (= assassin) use a calling card?

- \mathcal{P} sends to contract encryption (commitment) **e.CC** to calling card **CC** *before crime occurs*
- *After crime occurs*, \mathcal{P} opens **e.CC**, revealing **CC**
- Contract verifies that **CC** matches authenticated data feed
- Then **CC** proves \mathcal{P} committed crime!



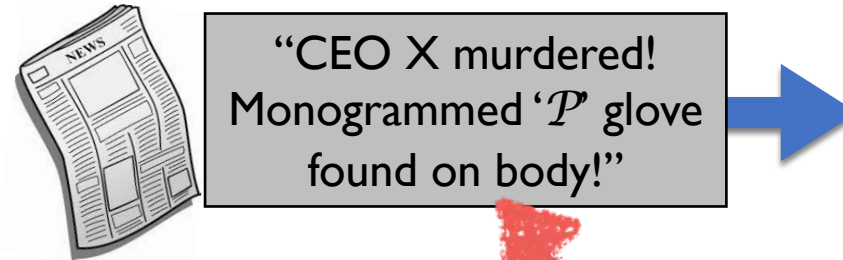
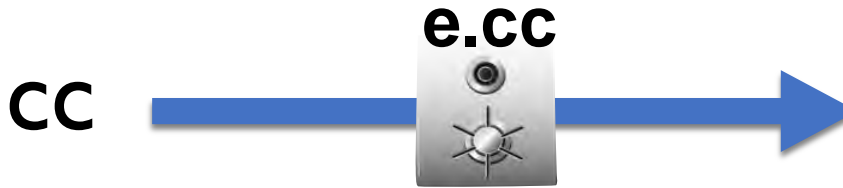


Full calling-card CSC

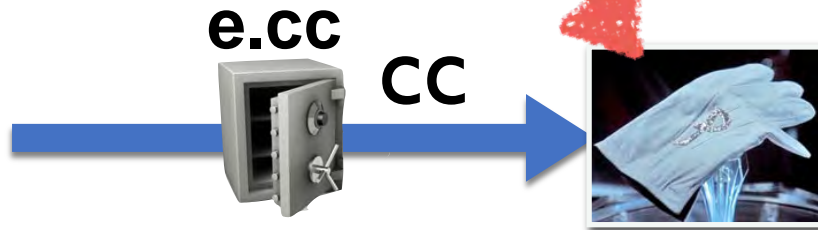
\mathcal{P} sends cc:



Authenticated news feed:



\mathcal{P} opens:



\mathcal{P} paid reward:



Assassination

\$1,000,000
reward for
CEO X

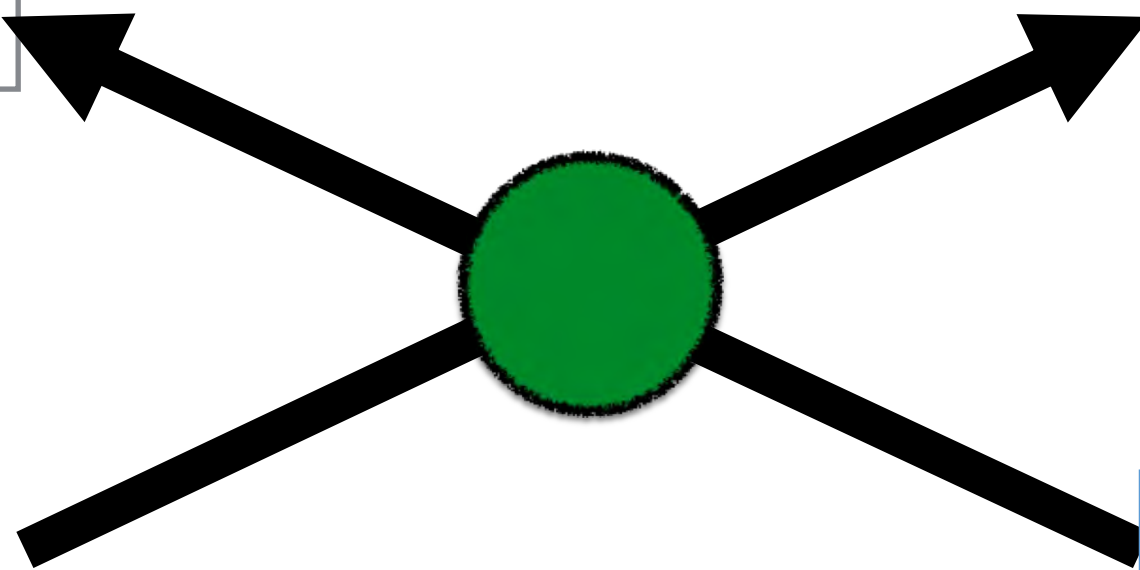


Commission fairness!

Contractor C

Perpetrator P

\$\$\$



I'd like to say that decentralized assassination markets will never happen, but...



Blockchain 101

Technology

Markets

Business

Data & Research

Consensus

Binance Reveals Plan to Launch Crypto Exchanges on Almost Every Cor



**The First Augur Assassination Markets
Have Arrived**

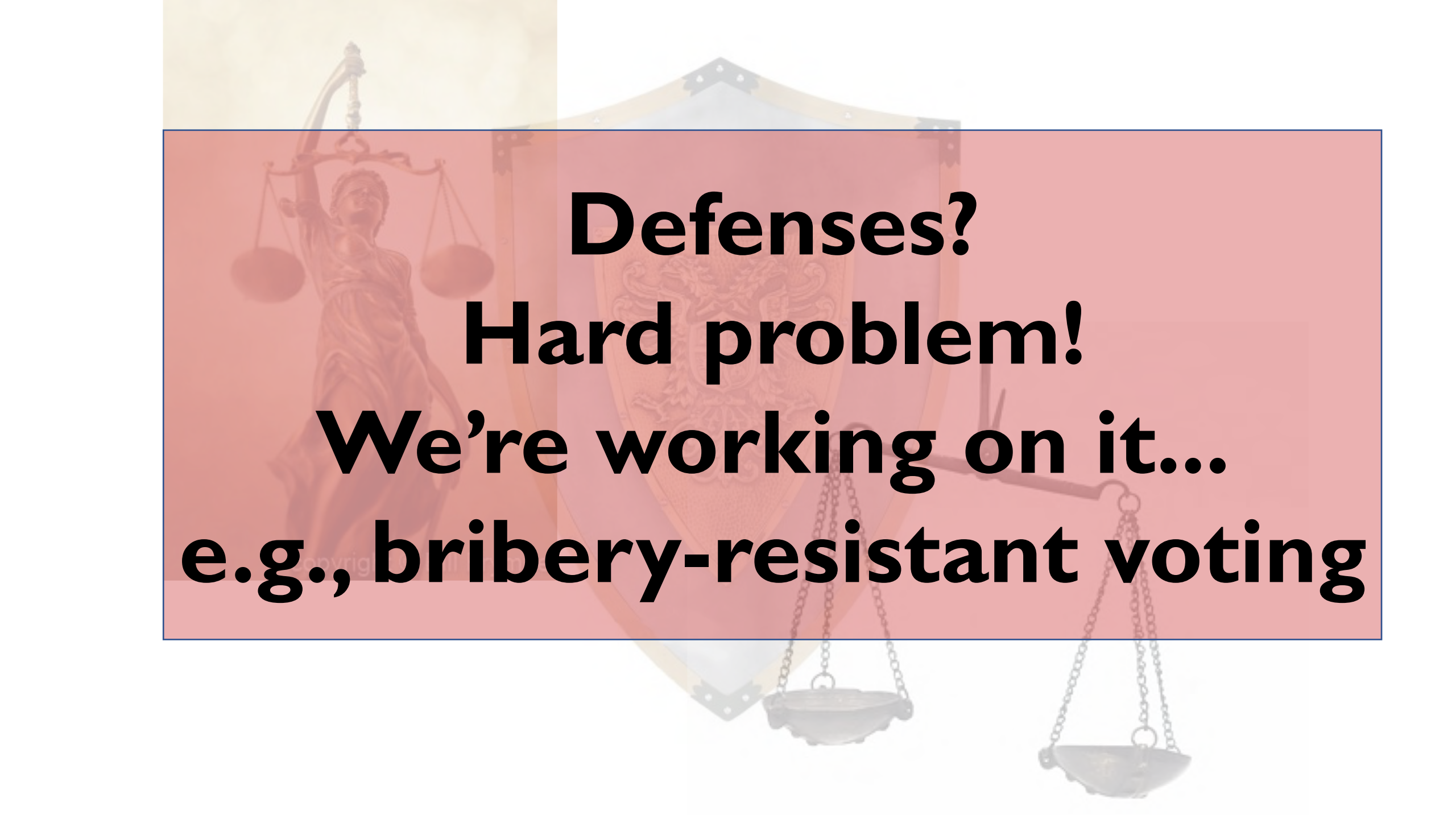
Assassination extreme, but CSCs for...

- Other physical crimes: arson, assault, etc.
- Cybercrimes:
 - leakage of data
 - theft of CA keys (in paper)
 - website defacement (in paper)

Note: For most CSCs, e.g., Assassination, *C* can just walk away!

Vote-buying

- Suppose Contract **A** is holding a vote
 - E.g., to decide whether to invest pools funds in Venture **V**
- Contract **B**(uyer) monitors Contract **A** and...
- If Address **X** sends “yes” vote to Contract **A**, then...
- Contract **B** sends \$I (in ETH) to **X**



Defenses?
Hard problem!
We're working on it...
e.g., bribery-resistant voting

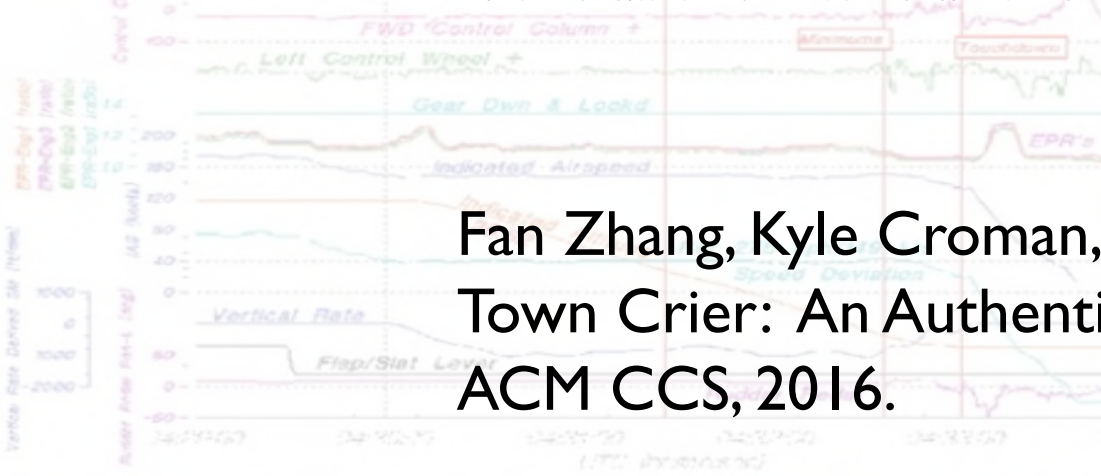
Enclave Creation – Details



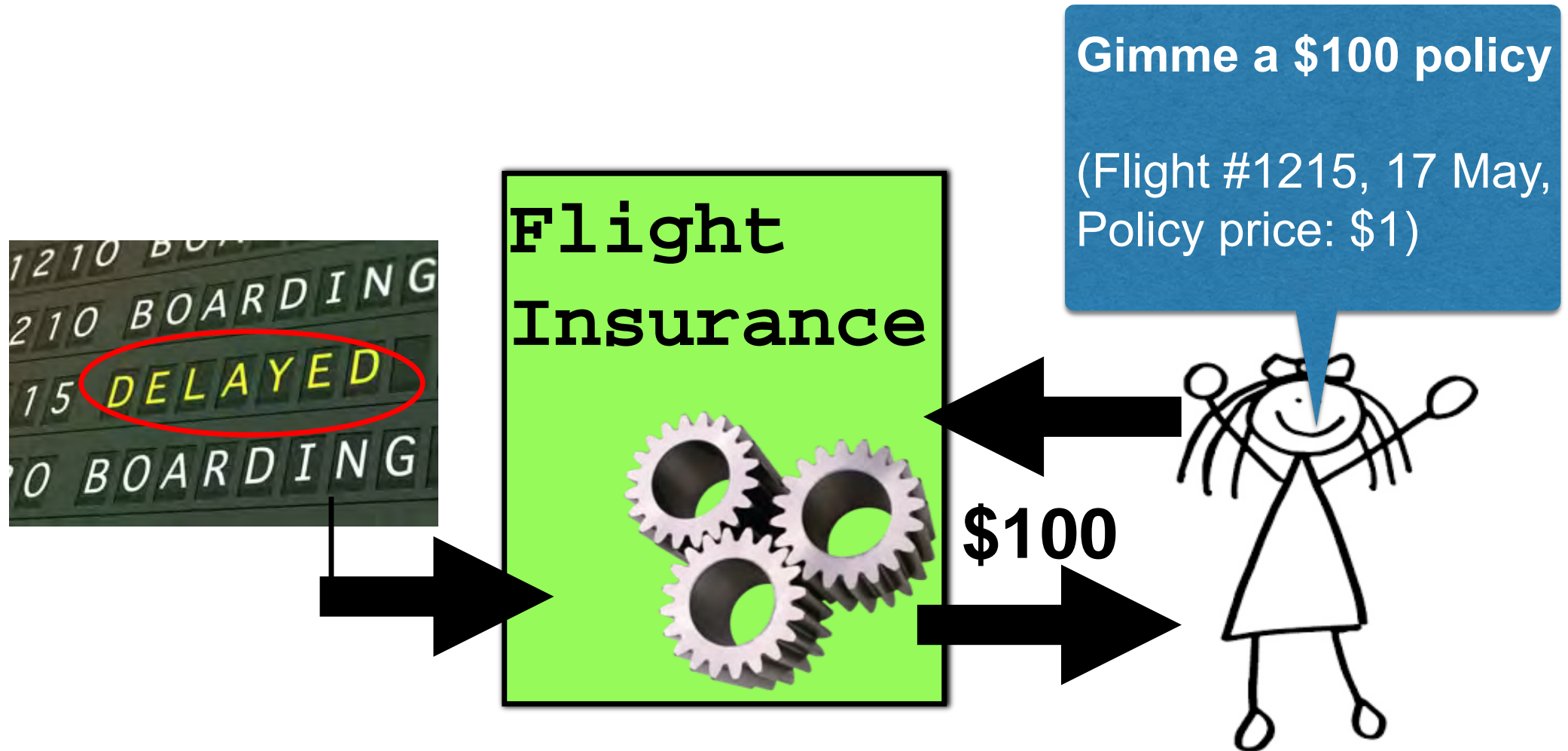
Town Crier



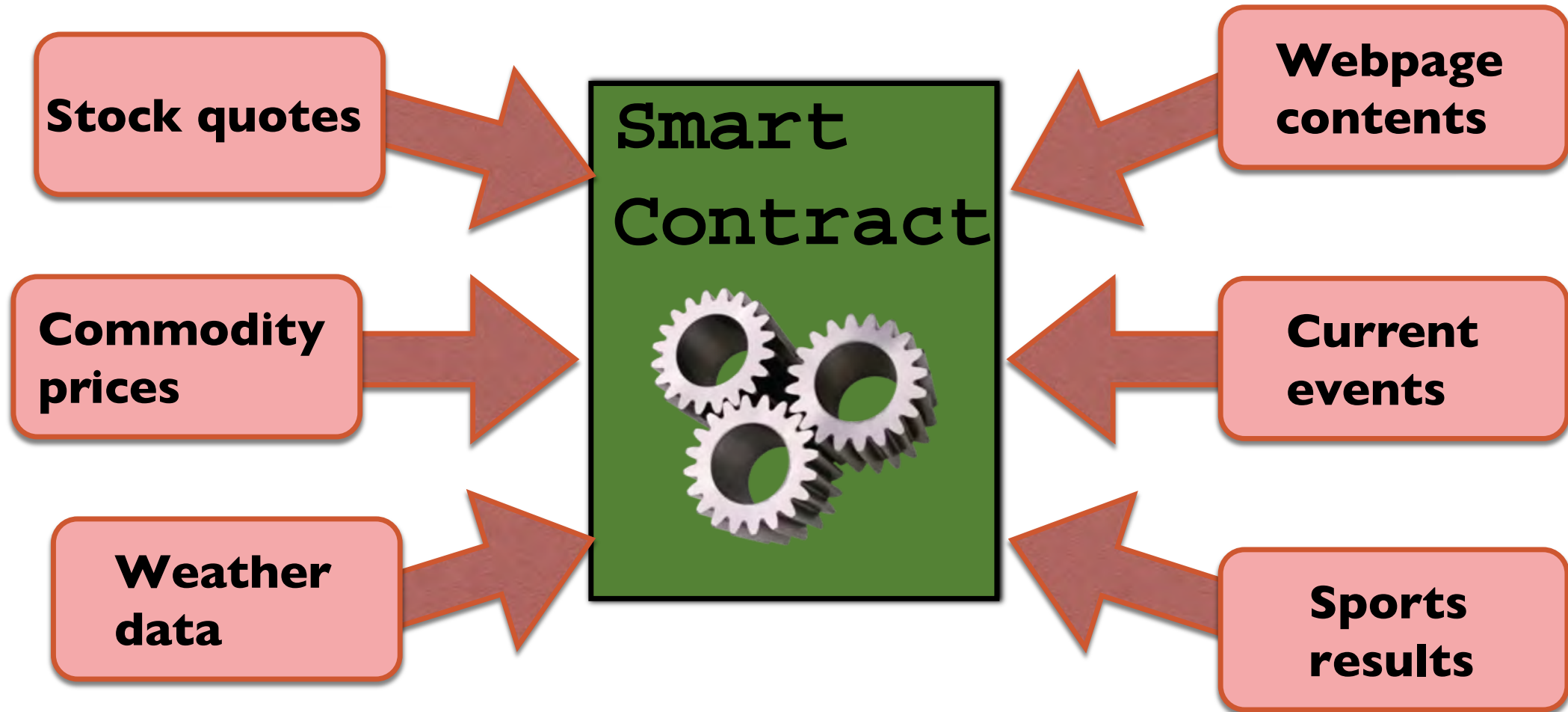
Fan Zhang, Kyle Croman, Ethan Cecchetti, Elaine Shi, and Ari Juels.
Town Crier: An Authenticated Data Feed for Smart Contracts.
ACM CCS, 2016.



Popular smart contract example



“Interesting” smart contracts are data hungry!



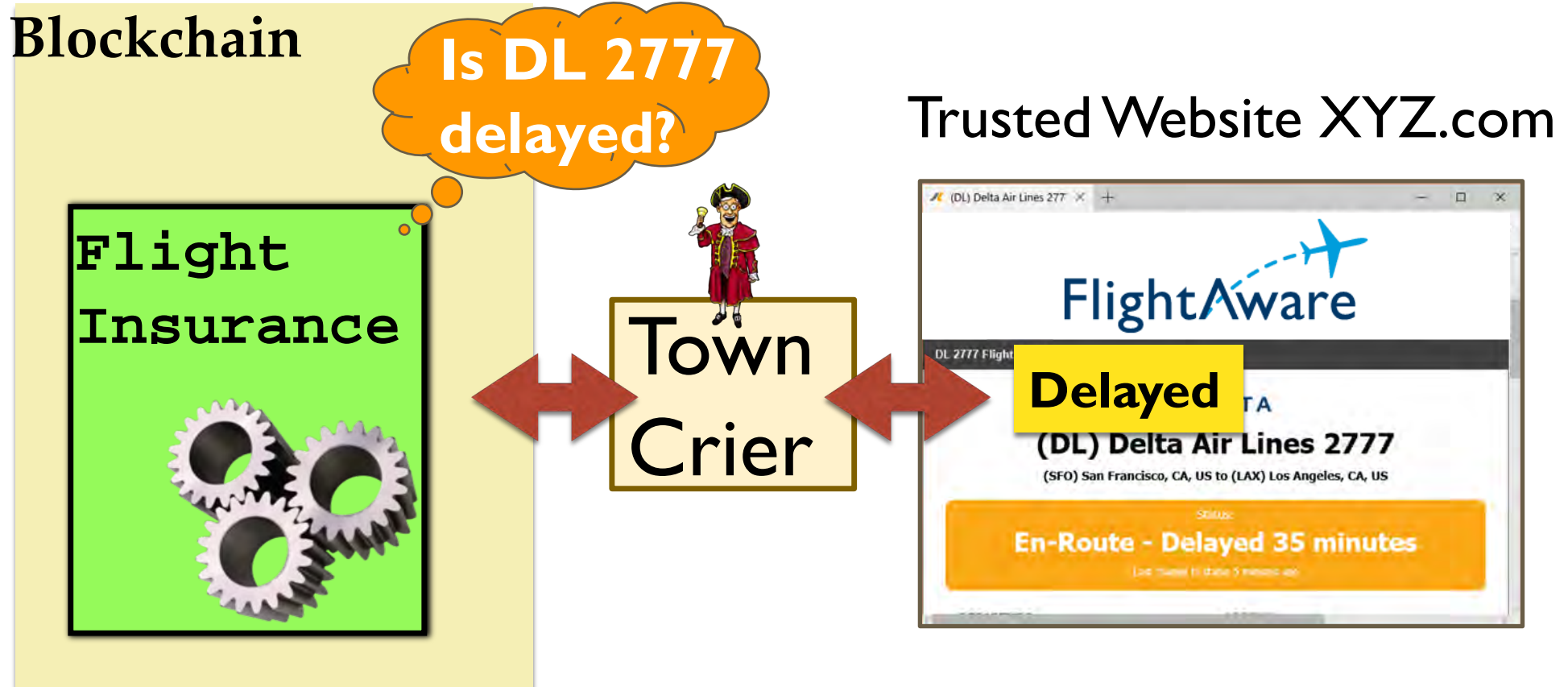
But smart contracts lack internet connections...

Blockchain

Flight
Insurance

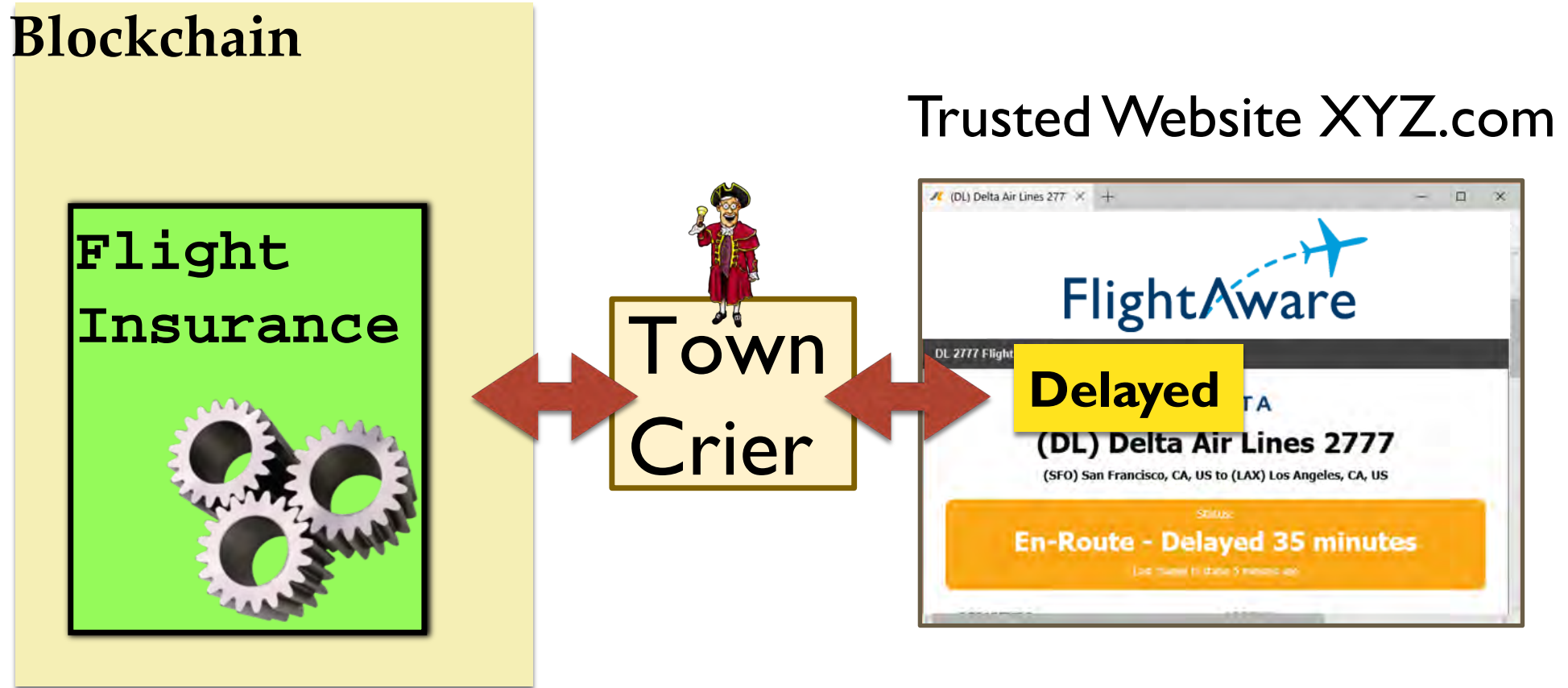


Town Crier (TC): Basic idea



Authenticity property: Data delivered by TC is exactly as served on source site XYZ.com

Town Crier (TC): Basic idea



But would you really trust a CT faculty member and PhD students to do this?

Town Crier (TC): Basic idea

Blockchain

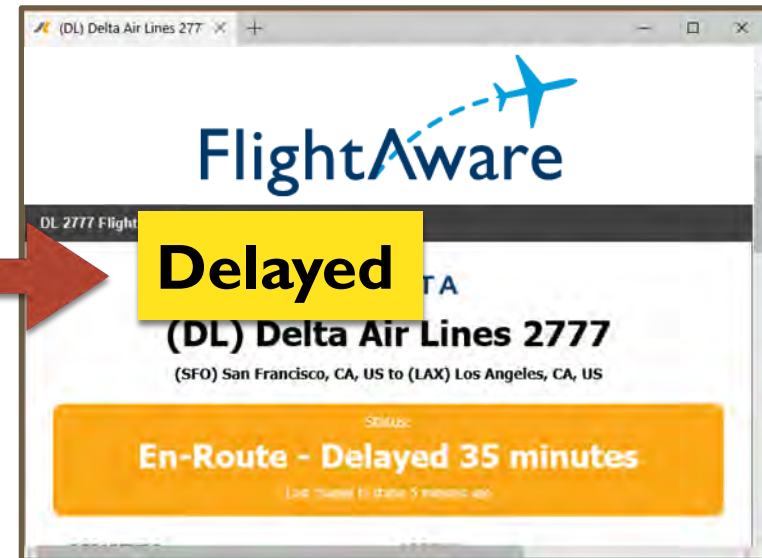
Flight
Insurance



Town
Crier

intel SGX

Trusted Website XYZ.com



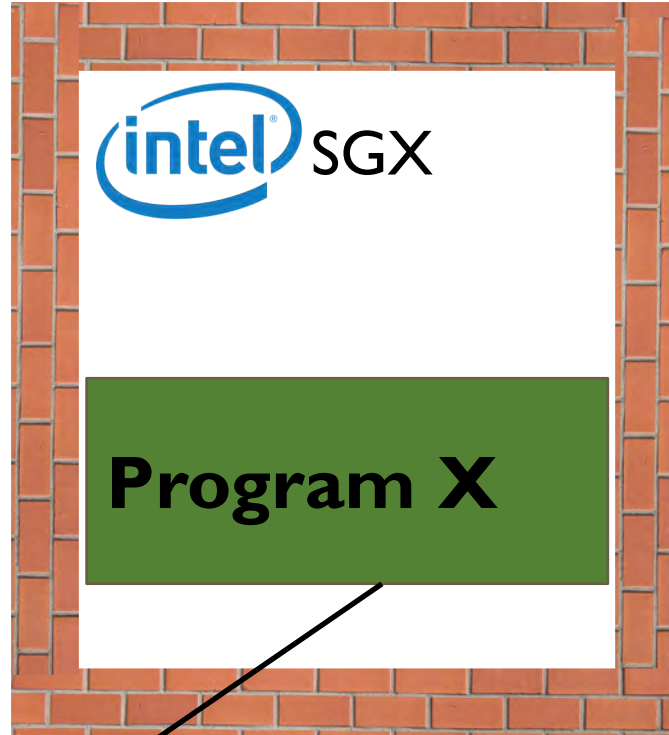
How to ensure TC *authenticity property*?

Intel SGX

Integrity



Other processes—
even OS—can't tamper
with control flow of X



Enclave

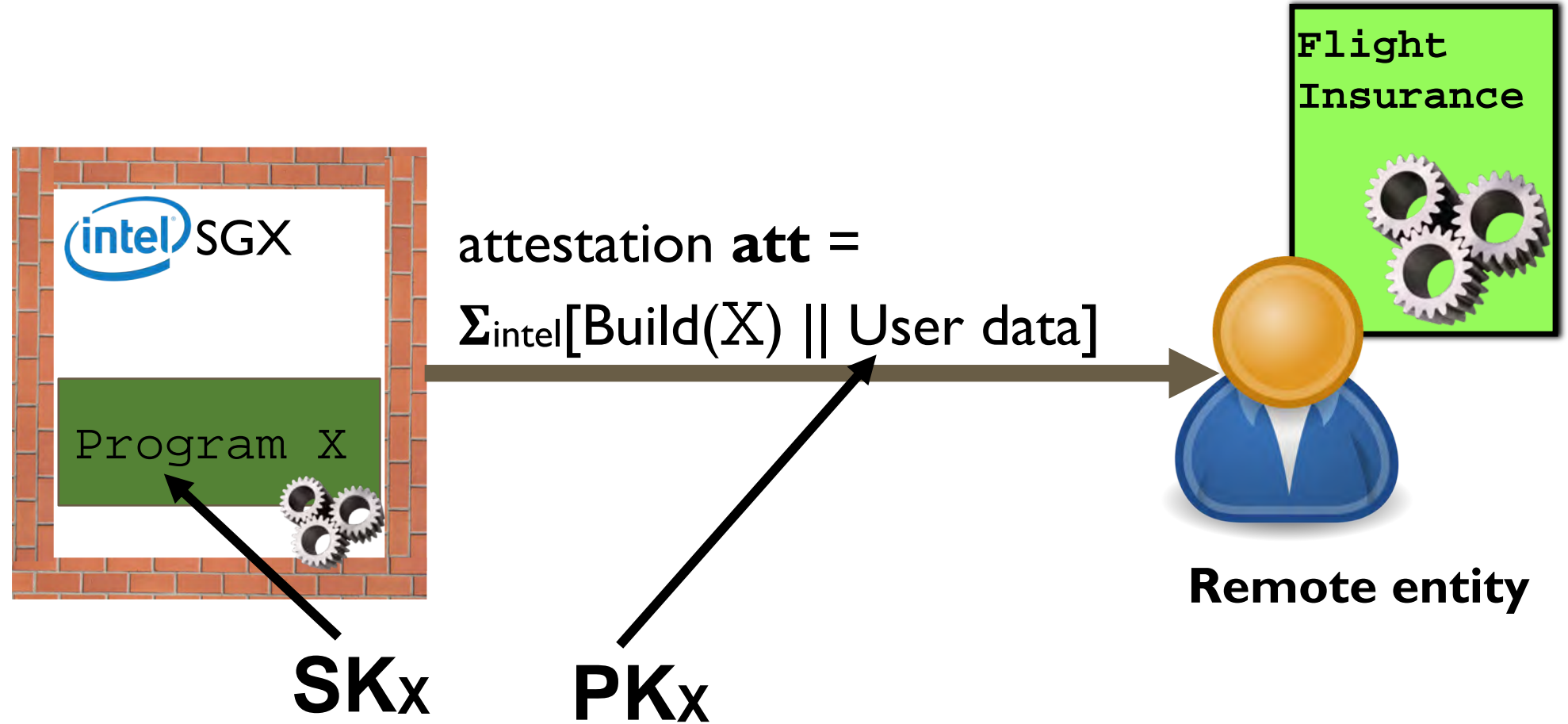
Confidentiality



Other processes—even
OS—learn nothing*
about state of X

* Excepting side-channels like page faults, cache, branch-shadowing

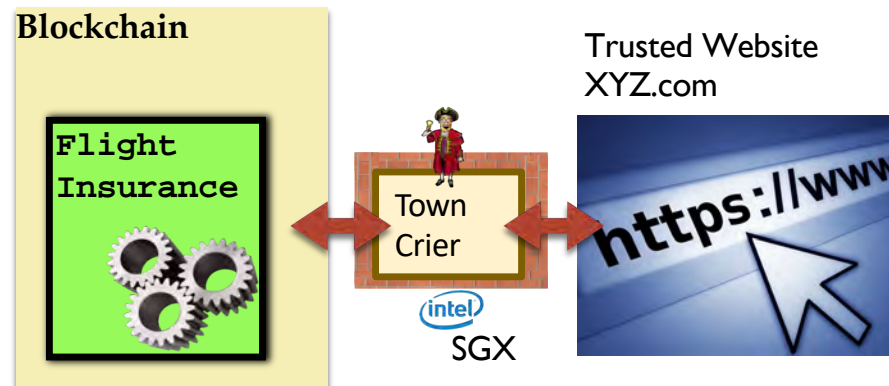
Intel SGX: Remote attestation



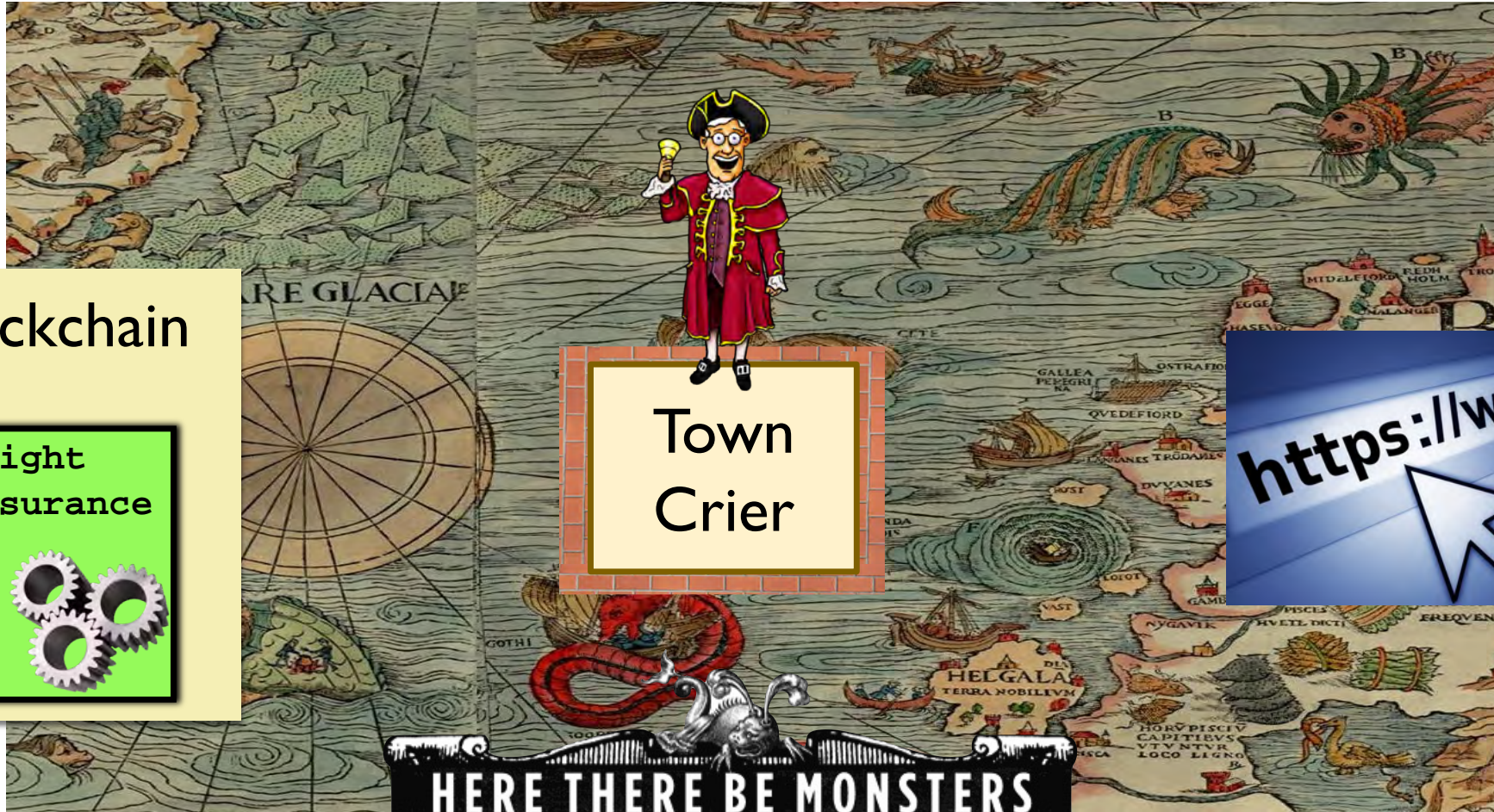
*Signature Σ (EPID) can be anonymous (group) or pseudonymous

TC goal / adversarial model

- Relying contract sends query $Q = (\text{XYZ.com}, \text{params}, T)$ to TC
- Goal: TC *authenticity property* for answer A to query Q
- Assumption: TC code trustworthy (publicly verified)
- *Adversary controls TC node OS and the network*



Our adversarial model...



Blockchain

Flight
Insurance



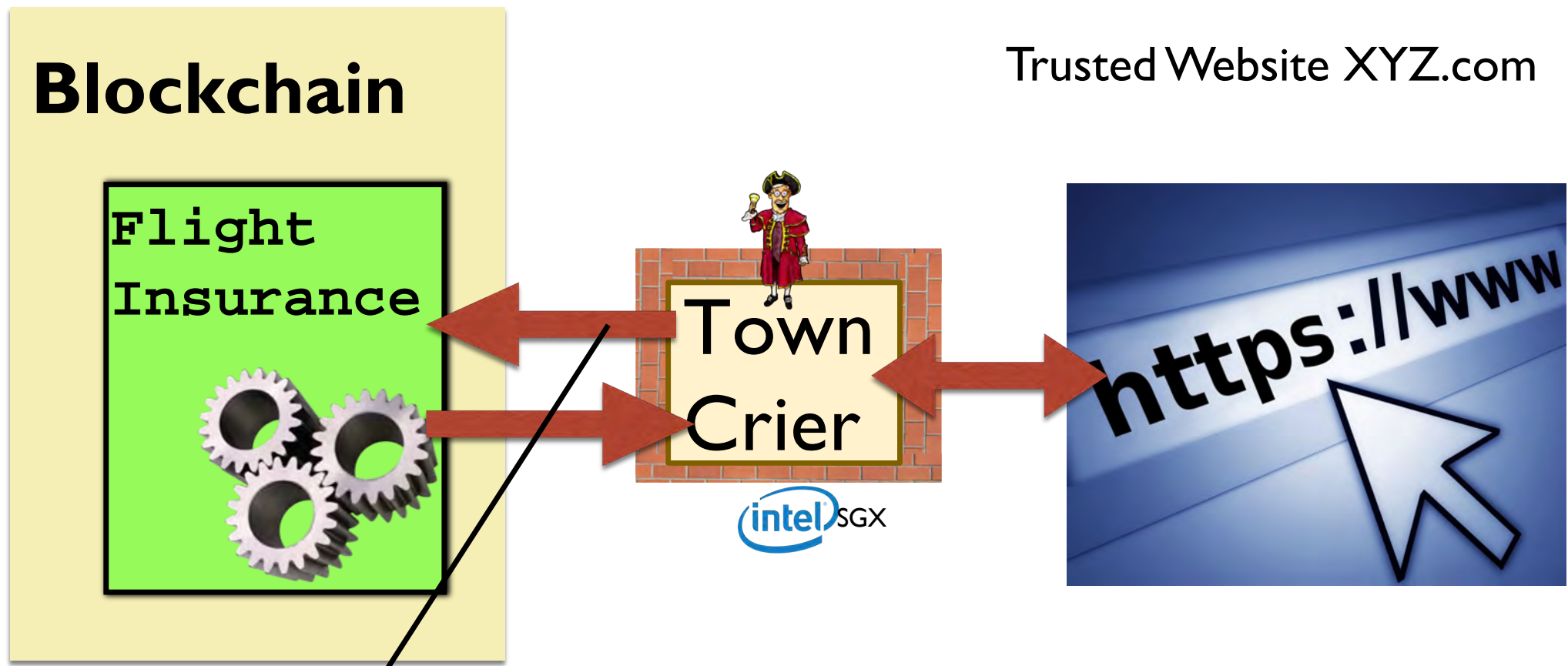
Town
Crier

<https://www>

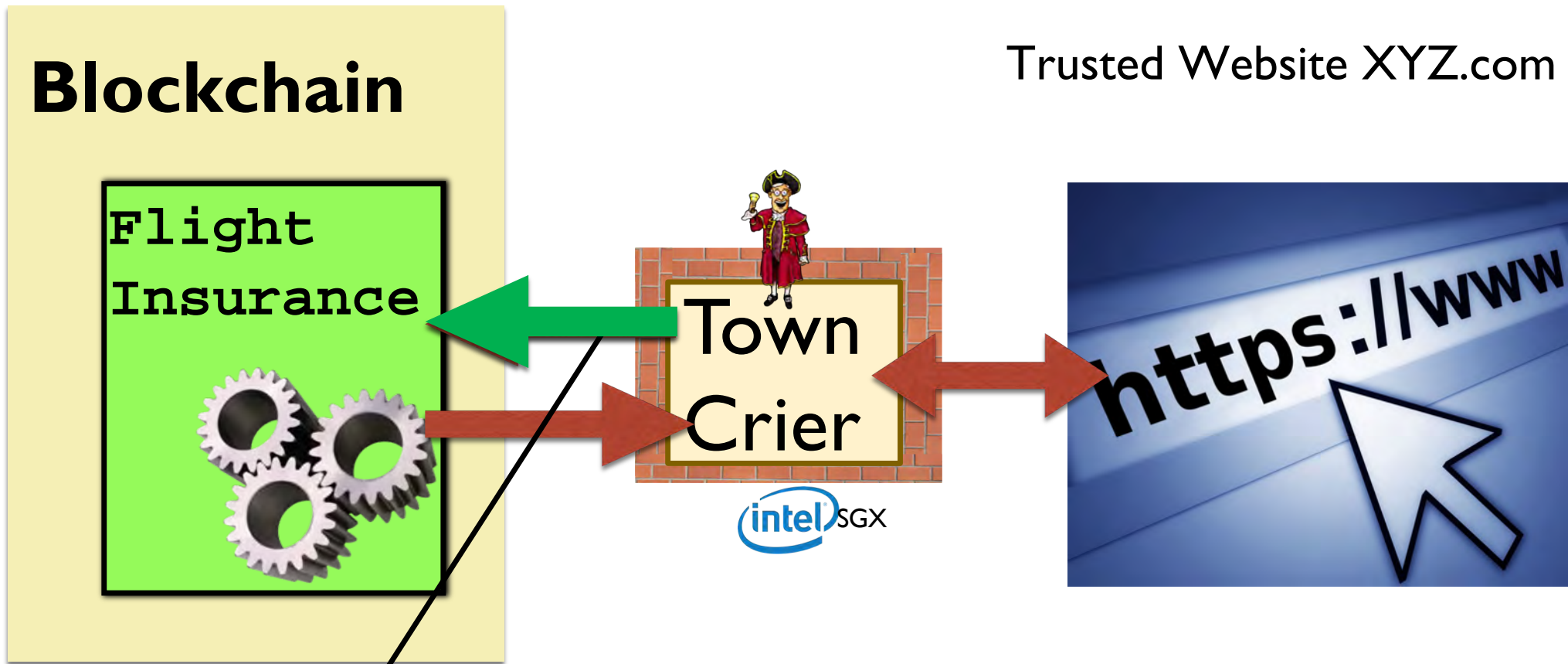
HERE THERE BE MONSTERS

DEALERS IN AND EXPORTERS OF RARE & ODD

Trusted
Website
XYZ.com



- TC source code is published
 - Anyone can compute TC_code
- Attestation generated: $\mathbf{att} = \Sigma_{\text{intel}}[\text{Build}(\text{TC_code}) \parallel \text{PK}_{\text{TC}}]$



(Simplified) steps for Flight Insurance :

- Creator checks **att** against TC_code , gets PK_{TC}
- Flight Insurance hardwired with PK_{TC}
- Flight Insurance checks signature $\Sigma_{SK_{TC}}[flight\ data]$ on flight data

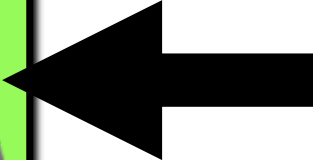
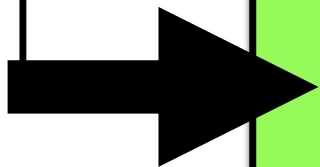
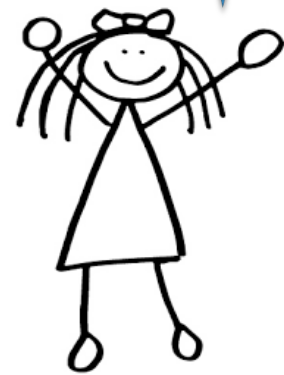
Another problem...



Flight Insurance

A green rectangular box containing the text 'Flight Insurance' at the top and three interlocking gears below it.

Gimme a \$100 policy
(Flight #1215, 17 May,
Policy price: \$1)

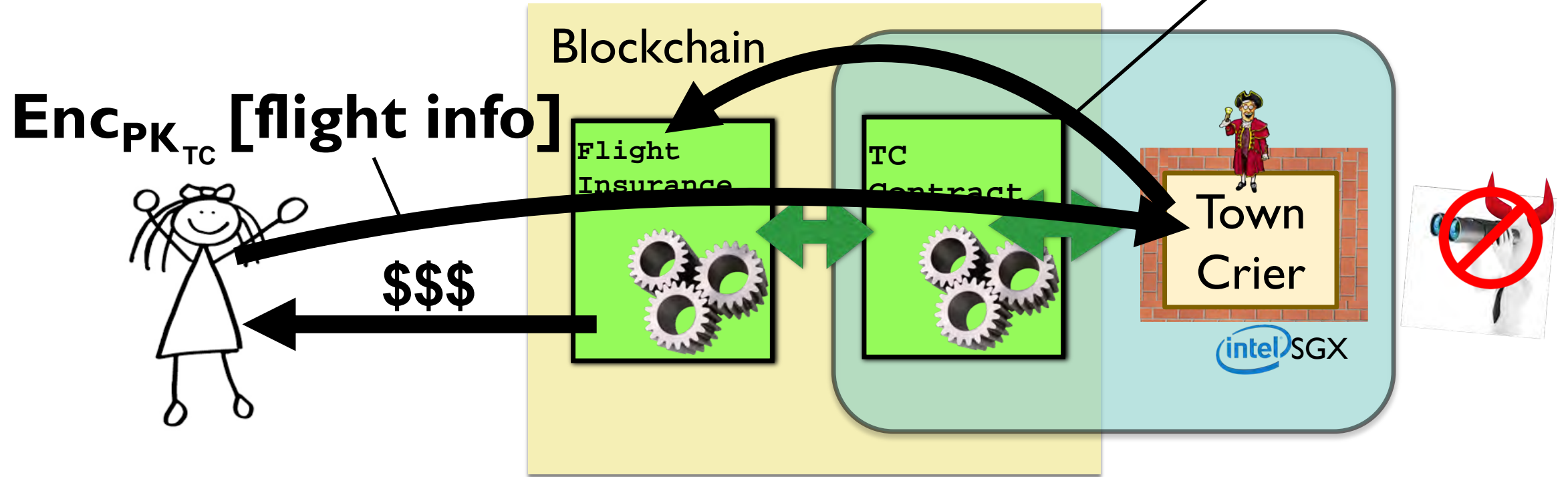


\$100



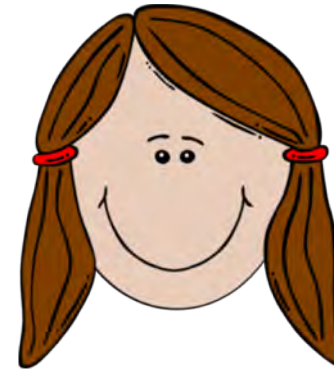
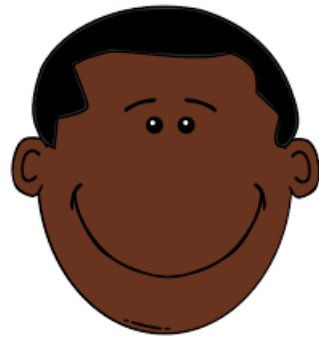
Town Crier offers data confidentiality

Flight delayed /
not delayed



...complex handling of private data possible

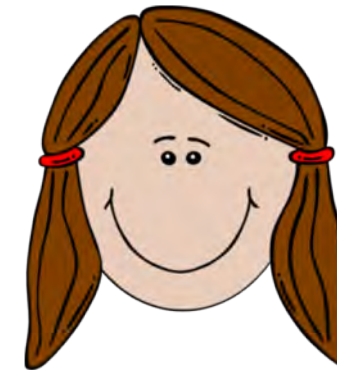
Application: New marketplaces for virtual goods



Other applications

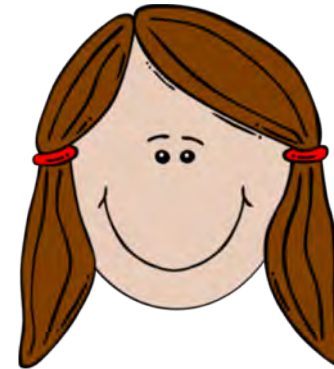
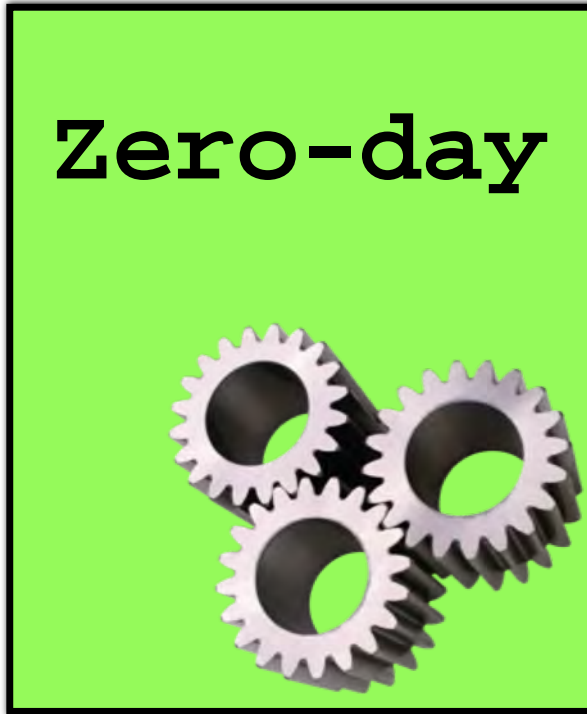
- All manner of financial instruments
- Many different types of insurance (flight, crop, etc.)
- Supply-chain management
- Etc., etc.

Fair marketplaces for bug-bounties



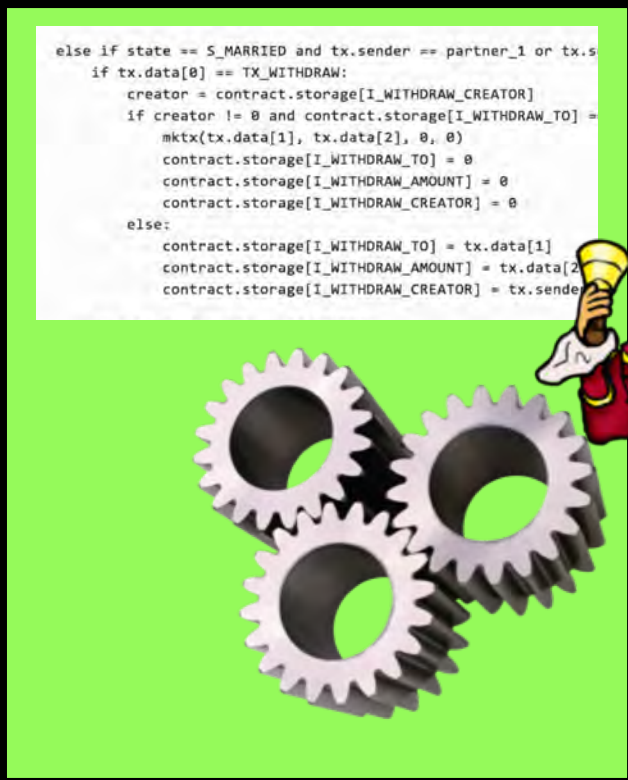
Florian Tramèr, Fan Zhang, Huang Lin, Jean-Pierre Hubaux, Ari Juels, Elaine Shi: Sealed-Glass Proofs: Using Transparent Enclaves to Prove and Sell Knowledge. IEEE Euro S&P 2017. To appear. (NSF-funded work)

Fair marketplaces for zero-days (sigh)



Town Crier Public Ethereum Launched: 15 May 2017

Special thanks to

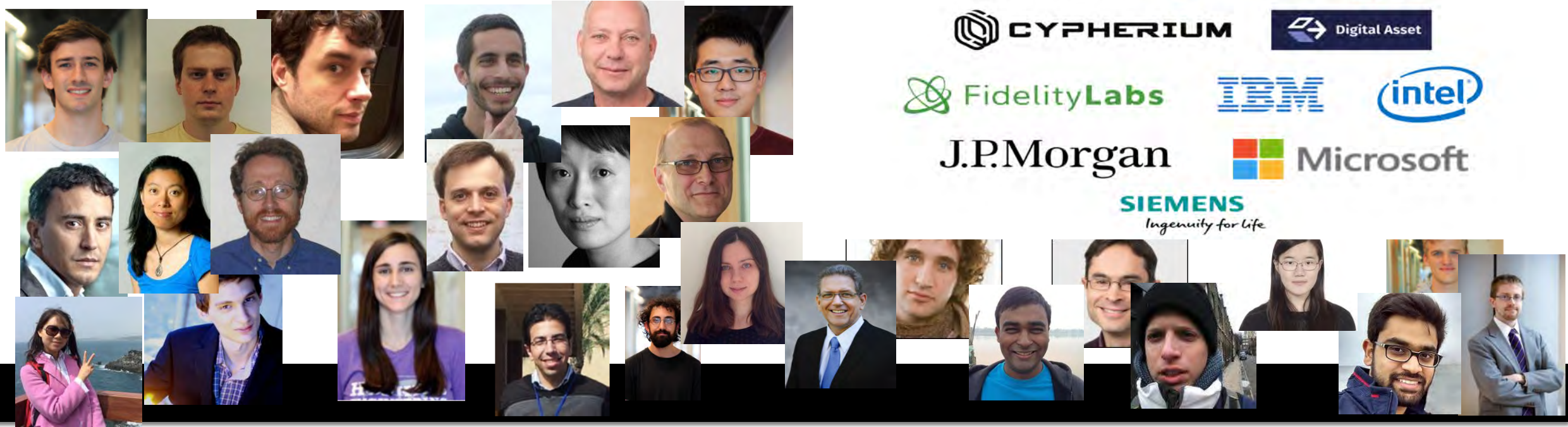


TC licensed to company this week...

```
else if state == S_MARRIED and tx.sender == partner_1 or tx.s  
if tx.data[0] == TX_WITHDRAW:  
    creator = contract.storage[I_WITHDRAW_CREATOR]  
    if creator != 0 and contract.storage[I_WITHDRAW_TO] =  
        mktx(tx.data[1], tx.data[2], 0, 0)  
        contract.storage[I_WITHDRAW_TO] = 0  
        contract.storage[I_WITHDRAW_AMOUNT] = 0  
        contract.storage[I_WITHDRAW_CREATOR] = 0  
    else:  
        contract.storage[I_WITHDRAW_TO] = tx.data[1]  
        contract.storage[I_WITHDRAW_AMOUNT] = tx.data[2]  
        contract.storage[I_WITHDRAW_CREATOR] = tx.sende
```



Initiative for CryptoCurrencies and Contracts (IC3)



www.initc3.org