The Jekyll and Hyde of Smart Contracts

Ari Juels
Jacobs Institute, Cornell Tech
Co-Director, IC3

Guest lecture, CS 5112
20 Sept. 2018
A Quick Blockchain + Bitcoin Refresher
Blockchains: Abstraction

Write Permission: Any valid data

Read Permission:
Bitcoin’s use of a blockchain

PK_A \rightarrow 2 \text{BTC} \rightarrow PK_B
Bitcoin’s use of a blockchain

Trans: 2 BTC: $PK_A \rightarrow PK_B$

$\text{Sig}\{SK_A, \text{Trans}\}$
Blockchain = Trusted (universal) memory

Trans: 2 BTC: PK_A → PK_B

Sig{SK_A, Trans}
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
Your personal files are encrypted

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.
Other Bitcoin-fueled mischief
Decentralized smart contracts will amp it all up
What's a Smart Contract?
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...

10 Bob’s Bubble Tokens (BBT) → 1 ETH

Problem of *Fair Exchange*!
Trusted third-party (with public state)
Smart contract ≈ Trusted third-party (with public state)
Plus, they’ll have oracles…
No, not Floyd Mayweather...
Floyd 'Crypto' Mayweather promotes an ICO, again

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
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
Simple smart contract: Lottery

**Init**:
- `T_{\text{end}} := 30 \text{ Sept 2018}`
- `$ticket := 1$`
- `pool := {}`
- `pot := 0$

**TicketPurchase**:
On receive `$amt` from party $P$:
- `Assert $amt = $ticket, balance[P] \geq $amt`
- `pot := pot + $ticket`
- `pool := pool \cup P`

**Timer**:
If $T > T_{\text{end}}$ then:
- `W \in R pool`

**Lottery Contract**

Contract Lottery
**Simple smart contract: Lottery**

**Contract Lottery**

**Init:**
\[
\begin{align*}
T_{\text{end}} & := 30 \text{ Sept 2016}, \\
$\text{ticket} & := 1, \\
\text{pool} & := \{\}, \\
\text{pot} & := 0
\end{align*}
\]

**TicketPurchase:**
On receive $amt$ from party $P$:
\[
\begin{align*}
\text{Assert } $amt & = $\text{ticket}, \text{ balance}[P] \geq $amt \\
\text{balance}[P] & := \text{balance}[P] - $\text{ticket} \\
\text{pot} & := \text{pot} + $\text{ticket} \\
\text{pool} & := \text{pool} \cup P
\end{align*}
\]

**Timer:**
If $T > T_{\text{end}}$ then
\[
\begin{align*}
W & \in \text{R pool} \\
\text{balance}[W] & := \text{balance}[W] + \text{pot}
\end{align*}
\]
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

1. 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 $\text{reward}$ (e.g., $\$1,000,000$) for assassination of CEO $X$

- How to verify:
  1. That assassination happened?
  2. That a claimed perpetrator $P$ was actually responsible?

- Solutions:
  1. Authenticated data feed / oracle
Assume…

Webpage contents

Sports

Weather

Smart Contract

Current events

Govt. documents

Commodity + equity prices
Contract: Assassination

• $C$ offers $\$\text{reward}$ (e.g., $\$1,000,000$) for assassination of CEO $X$

• How to verify:
  1. That assassination happened?
  2. That a claimed perpetrator $P$ 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)
How does $P$ (= assassin) use a calling card?

- $P$ sends to contract encryption (commitment) $e.cc$ to calling card $cc$ before crime occurs.
- After crime occurs, $P$ opens $e.cc$, revealing $cc$.
- Contract verifies that $cc$ matches authenticated data feed.
- Then $cc$ proves $P$ committed crime!
Full calling-card CSC

\(P\) sends cc:

Authenticated news feed:

\(P\) opens:

\(P\) paid reward:

Assassination

$1,000,000 reward for CEO X

“CEO X murdered! Monogrammed ‘P’ glove found on body!”
Commission fairness!

Contractor $C$

$\$$

Perpetrator $P$

$\$$
I’d like to say that decentralized assassination markets will never happen, but...
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 $1 (in ETH) to X
Defenses?
Hard problem!
We’re working on it...
e.g., bribery-resistant voting
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

Flight Insurance

Gimme a $100 policy
(Flight #1215, 17 May, Policy price: $1)
“Interesting” smart contracts are data hungry!

- Stock quotes
- Commodity prices
- Weather data
- Webpage contents
- Current events
- Sports results
But smart contracts lack internet connections...
Town Crier (TC): Basic idea

Blockchain

**Is DL 2777 delayed?**

Trusted Website XYZ.com

**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

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

Confidentiality

Other processes—even OS—learn nothing*

excepting side-channels like page faults, cache, branch-shadowing

* Excepting side-channels like page faults, cache, branch-shadowing
Intel SGX: Remote attestation

attestation $\text{att} = \Sigma_{\text{intel}}[\text{Build}(X) \ || \ \text{User data}]$

*Signature $\Sigma(EPID)$ can be anonymous (group) or pseudonymous*
TC goal / adversarial model

• Relying contract sends query \( Q = (\text{XYZ.com, params, } T) \) 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...
• TC source code is published
  • Anyone can compute $\text{TC\_code}$
• Attestation generated: $\text{att} = \Sigma_{\text{intel}}[\text{Build}(\text{TC\_code}) \ || \ \text{PK}_{\text{TC}}]$
(Simplified) steps for FlightInsurance:

- Creator checks **att** against **TC_code**, gets **PK_{TC}**
- FlightInsurance *hardwired* with **PK_{TC}**
- FlightInsurance checks signature **Σ_{SK_{TC}}[flight data]** on flight data
Another problem…

Gimme a $100 policy
(Flight #1215, 17 May, Policy price: $1)
Town Crier offers data confidentiality

...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

Fair marketplaces for zero-days (sigh)
Special thanks to

Town Crier Public Ethereum Launched:
15 May 2017
TC licensed to company this week...