BREAKING THE BLOCKCHAIN

Nadir Akhtar

ABOUT NADIR

- **UC Berkeley** graduate in CS, Dec 2019
- **Blockchain Security Intern** (soon to be Engineer) at **Coinbase**
- Former **Research Engineer** at **Quantstamp**
  - Contributed to a book on **smart contract security**
- Former **President** of Blockchain at Berkeley
- Led security consulting project for **Cred** via B@B
- Co-taught the Blockchain Fundamentals Decal (Largest blockchain student taught class in the world ~150 students)
  - Developed set of notes to accompany course, groundwork for book centered around cryptocurrencies and blockchain
  - edX instructor for course, totaling over 120,000 students around the world
- Taught in San Diego (Qualcomm), Taiwan, UC Berkeley I-School

LECTURE OUTLINE

1. WHAT IS BLOCKCHAIN SECURITY?
2. LAYER 1: THE BLOCKCHAIN
3. LAYER 2: THE APPLICATION
4. LAYER 3: THE INTEGRATION

1 WHAT IS BLOCKCHAIN SECURITY?

WHAT IS BLOCKCHAIN SECURITY?

AND WHY DO WE CARE?

BLOCKCHAIN: a linked list with hash pointers, primarily used in distributed and adversarial contexts to create and maintain a ledger of transactions
SECURITY: resistance to attackers

BLOCKCHAIN SECURITY: ensuring that a distributed ledger and supported applications correctly perform their jobs in the presence of adversaries/attackers

AUTHOR: NADIR AKHTAR

WHAT MAKES BLOCKCHAIN SECURITY SPECIAL?

AND WHY DO SO MANY PEOPLE LOSE MONEY?

COMPLEXITY: A blockchain involves several different mechanisms to function correctly and efficiently:

- Monetary policy
- Cryptography
- Consensus protocols
- Block propagation and networking procedures
- Programming languages
- Possibly more!

NASCENCY: The term “blockchain” as we know it has been around for hardly over a decade, and the startup mentality of “moving fast and breaking things” doesn’t play too well with blockchain’s permanence.

AUTHOR: NADIR AKHTAR

2 LAYER 1: THE BLOCKCHAIN

SECURING THE BLOCKCHAIN

Networking ➜ blockchain ➜ applications ➜ integrations

SECURING THE BLOCKCHAIN

THE SOURCE OF TRUTH

What do we need?

- Some concept of success
  - What does our blockchain aim to achieve?
- Principles to adhere to
  - Do we favor safety or liveness? Do we prefer simplicity and safety or accept the risks that come with feature-rich complexity?
- A consensus protocol
  - How do our different machines agree on what we care about?
  - An incentive scheme is almost always necessary when dealing with untrusted peers

SECURING THE BLOCKCHAIN

WHAT IS SUCCESS?

Do we want to:

- Create a decentralized currency?
- Enable decentralized, trustless computation?
- Track identities/voting?
- Put computational power towards research?
- Or something else?

SECURING THE BLOCKCHAIN

WHAT TRADEOFFS DO WE MAKE?

Do we prioritize:

- Safety or liveness?
- Security or complexity?
- Supply or demand?
- Trustless or limited?

SECURING THE BLOCKCHAIN

HOW DO WE BUILD OUR SYSTEM?

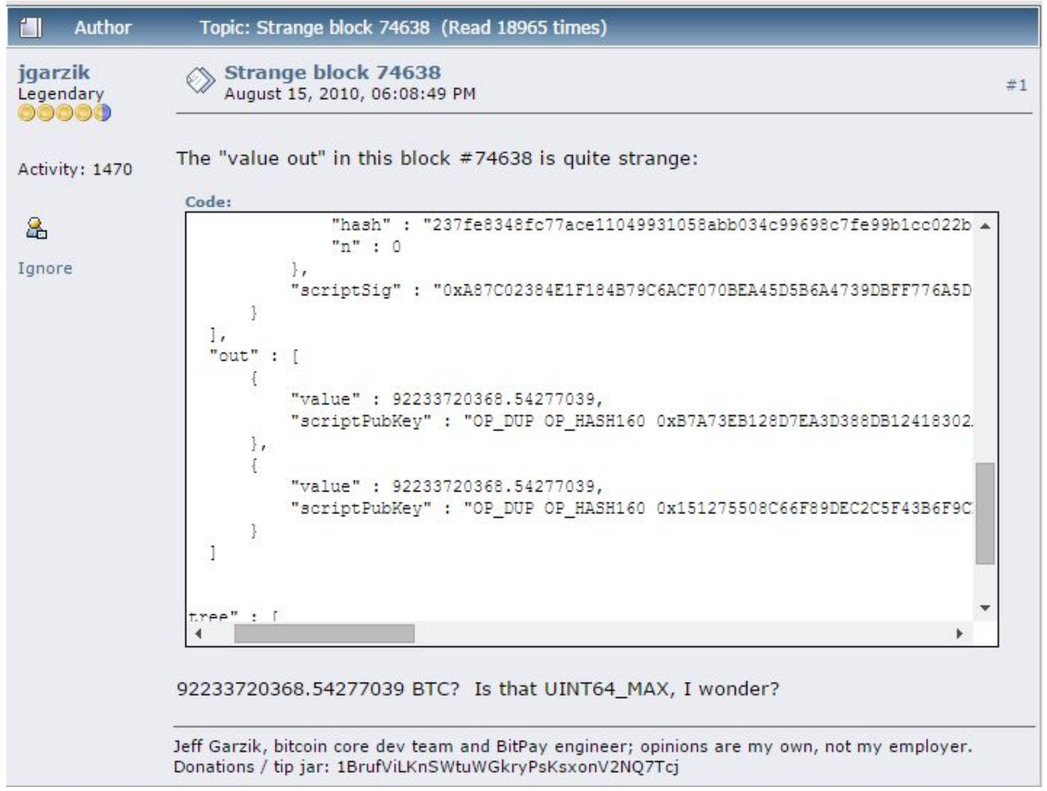
Do we prefer:

- Synchronous or asynchronous?
- Finality or mutability?
- Nakamoto-style or BFT-style?
- Specialized or generic resources?

BLOCKCHAIN-LEVEL BUGS

HOW DO WE BUILD OUR SYSTEM?

Overflow in Bitcoin!



Author | Topic: Strange block 74638 (Read 18965 times)

jgarzik
Legendary

Strange block 74638
August 15, 2010, 06:08:49 PM #1

Activity: 1470

Ignore

The "value out" in this block #74638 is quite strange:

Code:

```
            "hash" : "237fe8348fc77ace11049931058abb034c99698c7fe99b1cc022b
            "n" : 0
        },
        "scriptSig" : "0xA87C02384E1F184B79C6ACF070BEA45D5B6A4739DBFF776A5D
    }
],
"out" : [
    {
        "value" : 92233720368.54277039,
        "scriptPubKey" : "OP_DUP OP_HASH160 0xB7A73EB128D7EA3D388DB12418302
    },
    {
        "value" : 92233720368.54277039,
        "scriptPubKey" : "OP_DUP OP_HASH160 0x151275508C66F89DEC2C5F43B6F9C
    }
]

tree" : [
```

92233720368.54277039 BTC? Is that UINT64_MAX, I wonder?

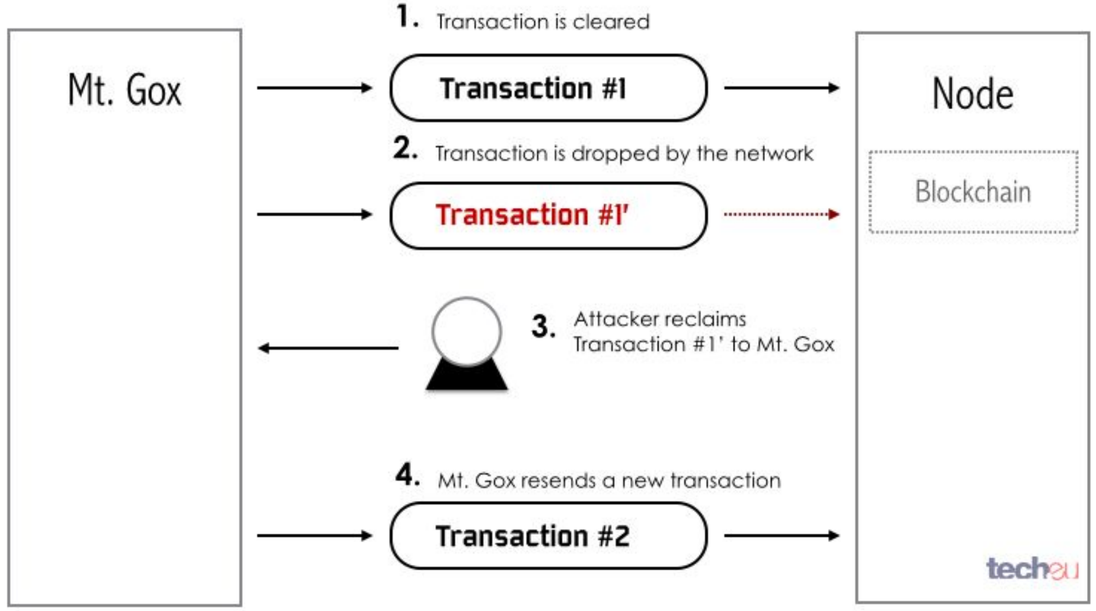
Jeff Garzik, bitcoin core dev team and BitPay engineer; opinions are my own, not my employer.
Donations / tip jar: 1BrufViLKnSWtuWGkryPsKsxonV2NQ7Tcj

Source: Bitcoin Core Bugs - The Evolution of Bitcoin Scripting Interpreter

BLOCKCHAIN-LEVEL BUGS

HOW DO WE BUILD OUR SYSTEM?

Transaction malleability!



Source: A Guide to Bitcoin (Part II): A deep dive into the Bitcoin ecosystem

3 LAYER 2: THE APPLICATION

SECURING THE BLOCKCHAIN

Networking → blockchain → applications → integrations

DAO HACK

What is DAO (Decentralized autonomous organization)

- Virtual venture capital (VC) fund that is governed by the investors of the DAO
- Main Idea:
  - Token holders can become contractors by submitting proposals for funding of their project by using the DAO funds
  - Proposals are approved by a quorum of 20% of all tokens
    - Transfers Ether automatically to the Smart Contract that represents the proposal
  - Raised 12.7 mil. Ether (150 mil USD in June 2016)
  - BUT...they got **H A C K E D**.

AUTHOR: JANICE NG

DAO HACK

What was the HACK?

“SPLIT PROCEDURE”, THE CATALYST OF THE HACK.

- The creators of DAO implemented the ability of a DAO to be split into 2
- “Minority” = able to retrieve funds when a proposal they objected gets approved
  - At least 48 days before getting it in an account YOU control

THE HACK:

- Coder found a loophole in this procedure
  - Once a split function is called, the code was written in a way to **retrieve ether → update balance**
  - Recursively call the “split procedure” and retrieve their funds **multiple times** before getting to the step where the **code checked the balance**
  -

RESULT OF THE HACK:

- On June 16, 2016, the attacker retrieved **~3.6 million Ether = 150 mil. USD**
- Now known as, the **“recursive call exploit”**

AUTHOR: JANICE NG

PARITY

TWO WRONGS DON'T MAKE A RIGHT

Parity is a company responsible for multiple "core blockchain" solutions, such as:

- A multisig wallet
- An Ethereum client
- Polkadot, for interoperable blockchains

We'll talk about how the first one, the wallet, got popped... twice.

WHAT IS A MULTISIG WALLET?

TWO WRONGS DON'T MAKE A RIGHT

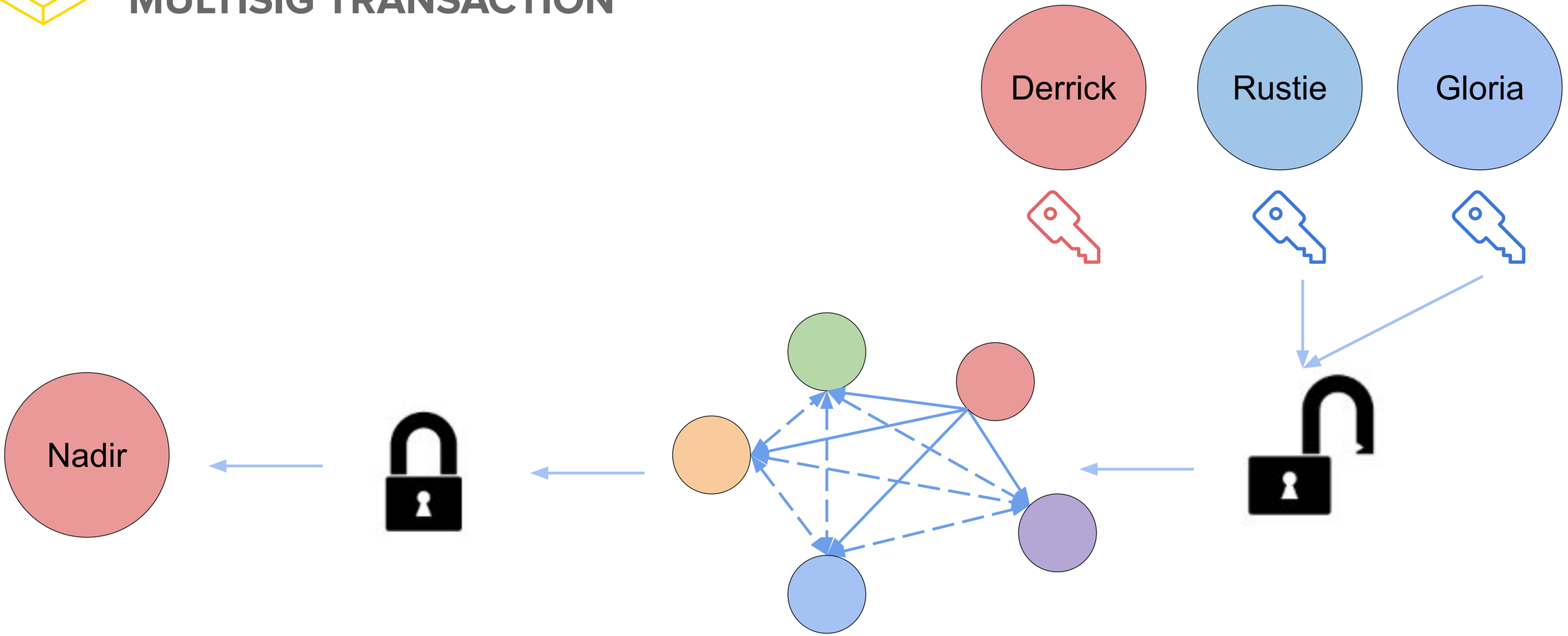
A multisig wallet exists to allow for a single account to allow for multiple users to produce valid signatures from that account, requiring a minimum threshold.

For example, a 2-of-3 multisig wallet requires 2 signatures from a total of 3 privileged users.

AUTHOR: NADIR AKHTAR

BITCOIN MECHANICS

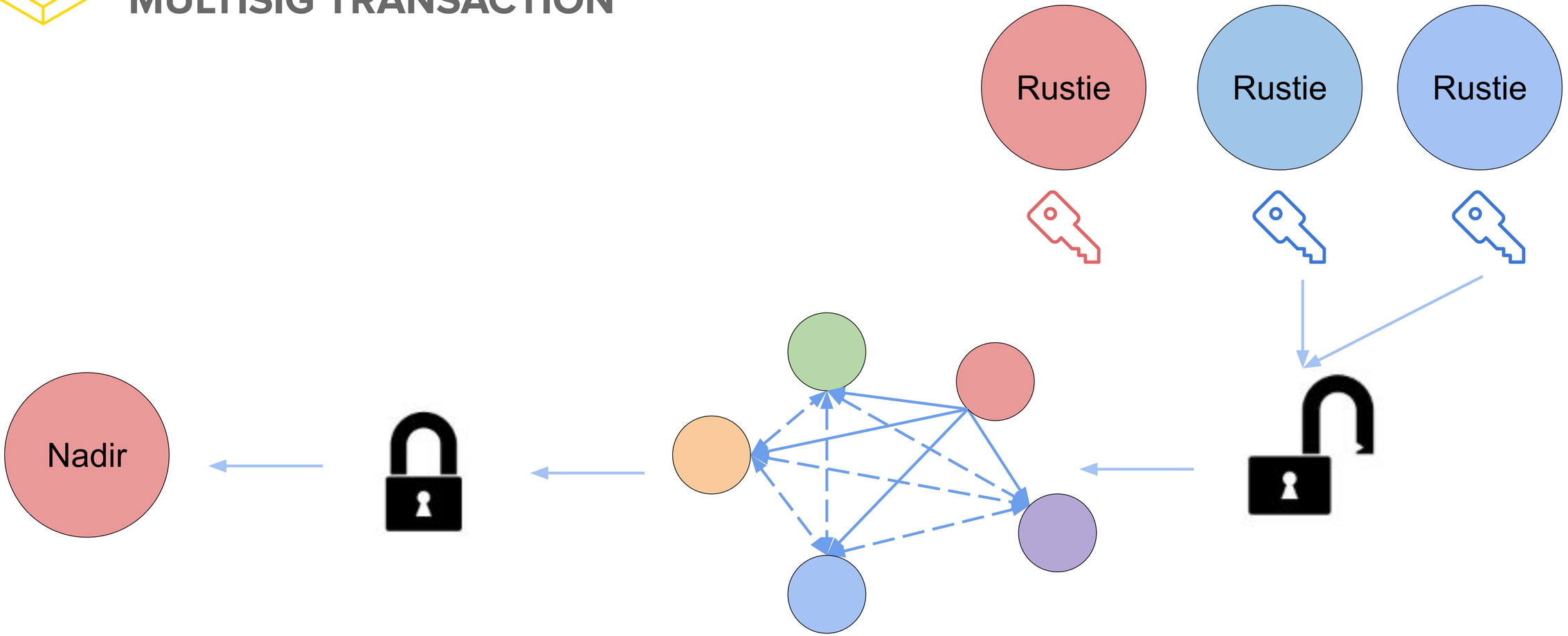
MULTISIG TRANSACTION



AUTHOR: RUSTIE LIN

BITCOIN MECHANICS

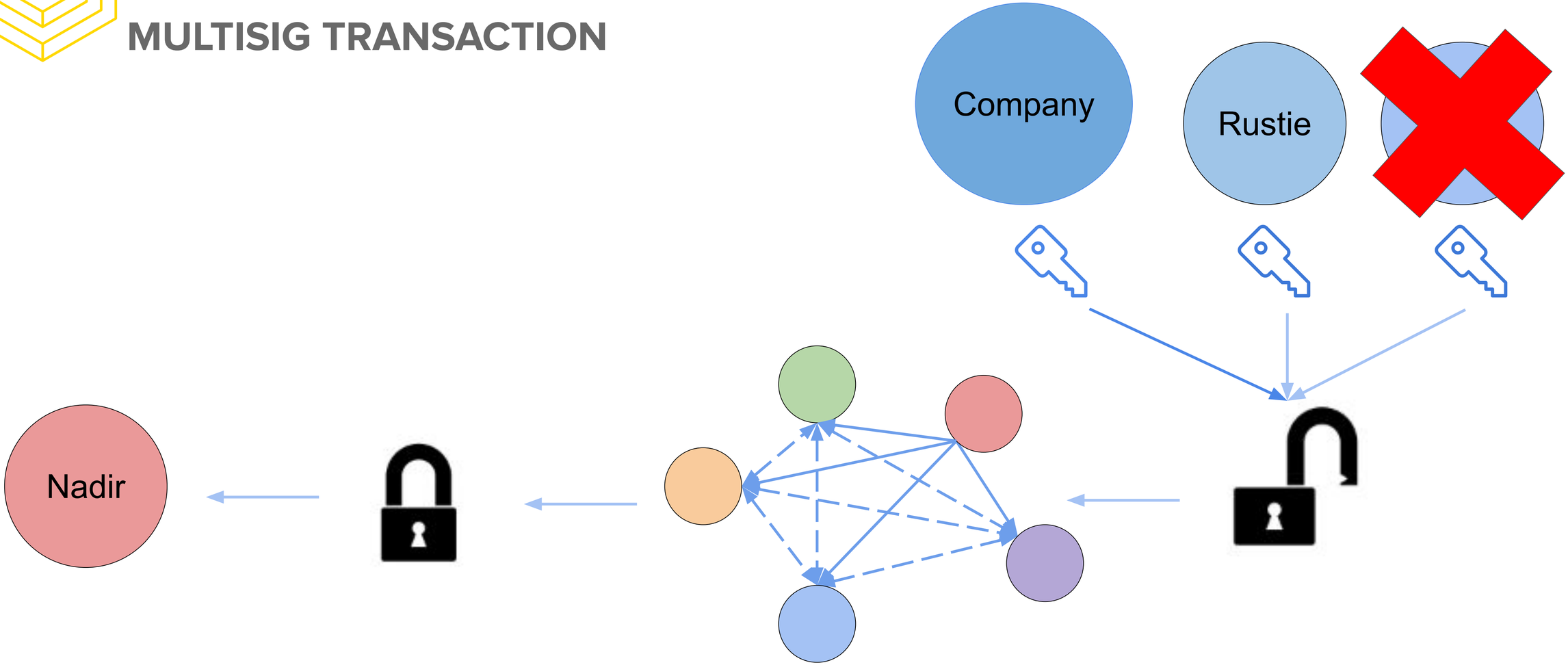
MULTISIG TRANSACTION



AUTHOR: RUSTIE LIN

BITCOIN MECHANICS

MULTISIG TRANSACTION



AUTHOR: RUSTIE LIN

MULTISIG WALLET HACK #1

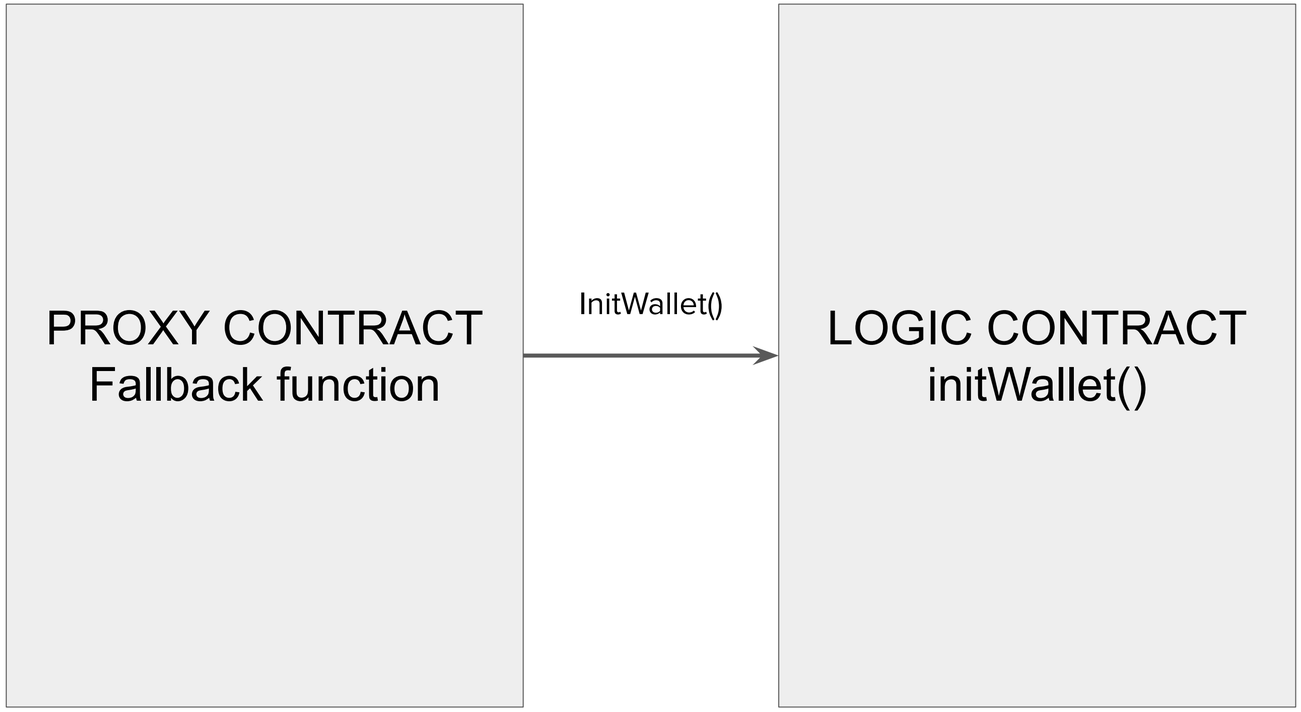
THE DANGERS OF FALLBACK FUNCTIONS

Contract design:
- Proxy contract as interface
- Logic contract to hold the actual logic (library contract)

An attacker made two calls:
- One to a fallback function
- The other to redeem funds

The fallback function would delegate arbitrary calls to the logic contract
- Beware “arbitrary”!

The initWallet function could be called more than once... requiring a National Treasure whitehat rescue



Source: The Parity Wallet Hack Explained

MULTISIG WALLET HACK #2

THE DANGERS OF CROSS-CONTRACT CALLS

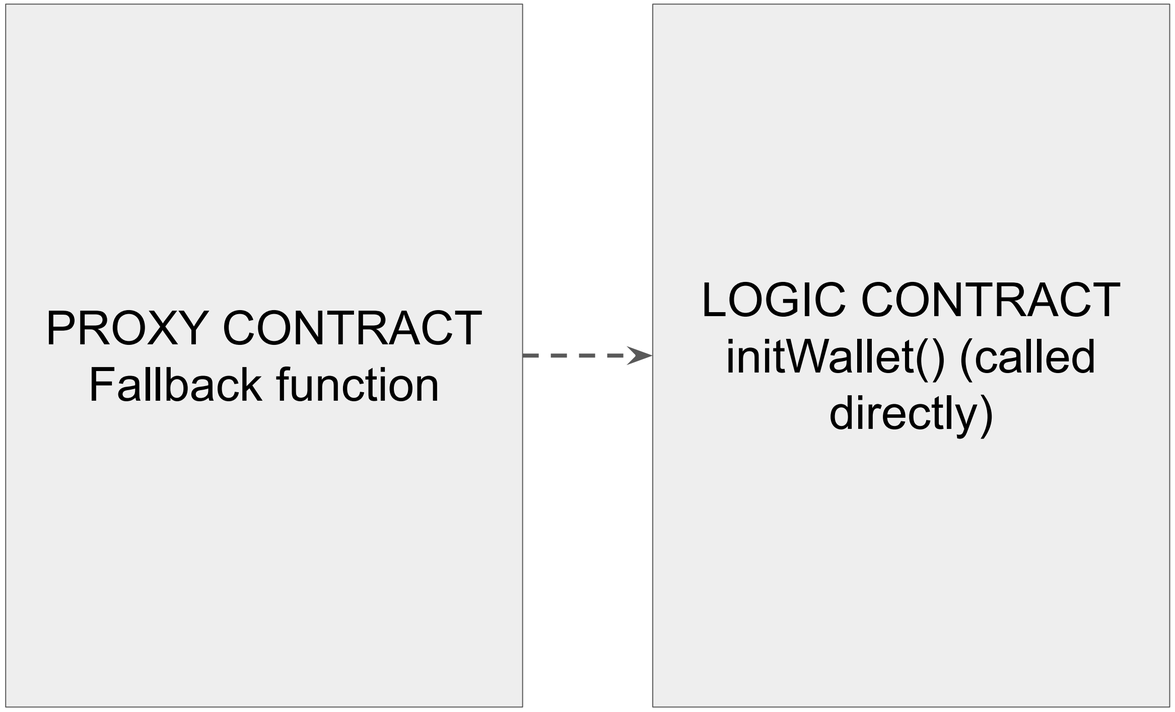
The previous fix? Add a modifier to ensure that it has not been initialized

The consequence? No one initialized the logic contract!

The logic contract was:

1. Directly called and initialized
2. Self-destructed (“killed”)

Now all proxy contracts are useless, meaning all funds held are frozen



Source: The Parity Wallet Hack Reloaded

AUTHOR: NADIR AKHTAR

4 LAYER 3: THE INTEGRATION

SECURING THE BLOCKCHAIN

Networking ➜ blockchain ➜ applications ➜ integrations

SECURING THE BLOCKCHAIN

"TRADITIONAL" APPLICATION SECURITY

Doesn't require blockchain knowledge!
(though it helps)

Includes:

- SQL injection
- Cross site scripting
- Cross site request forgery
- Server side request forgery
- And more!

SECURING THE BLOCKCHAIN

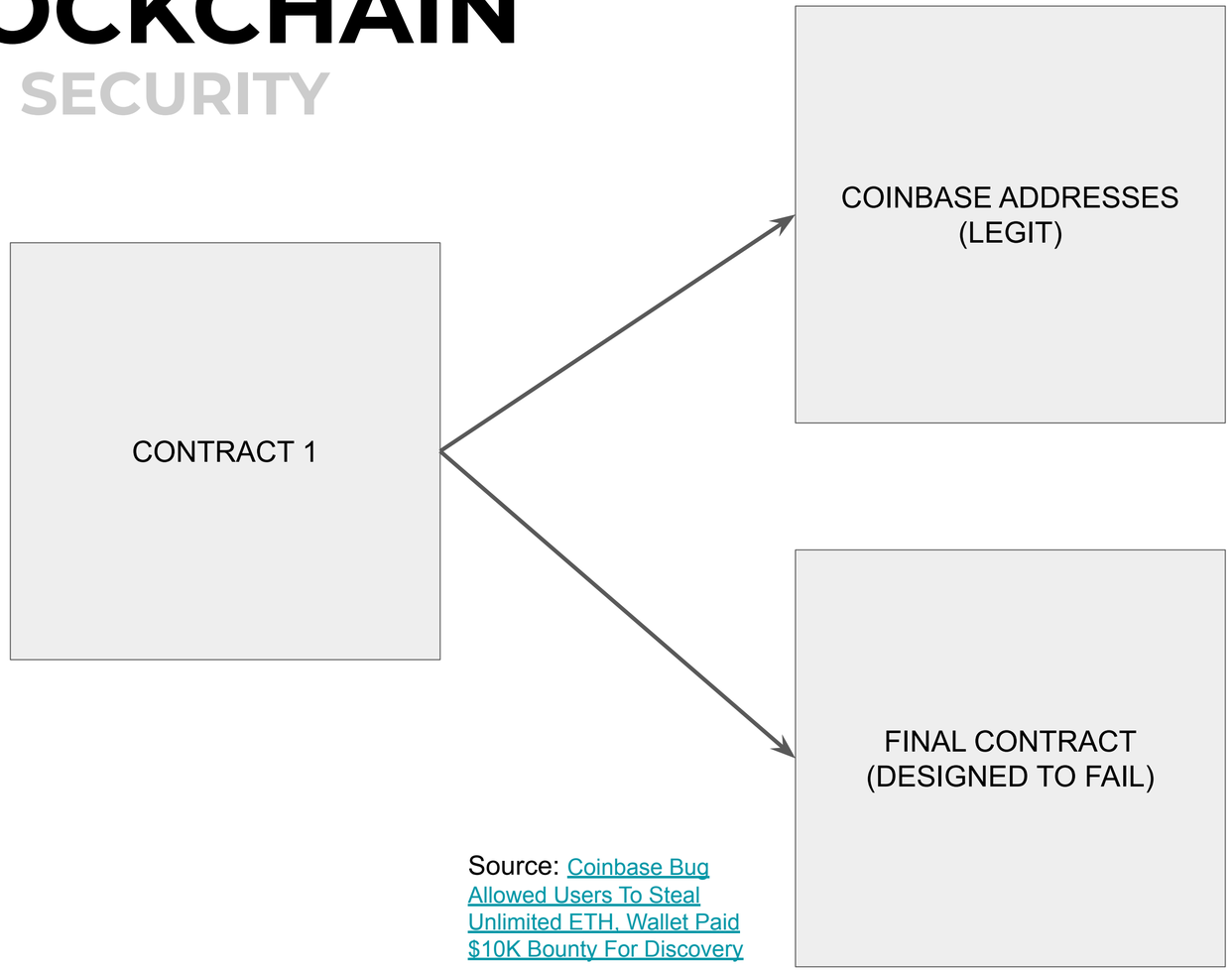
"TRADITIONAL" APPLICATION SECURITY

Coinbase is an exchange for cryptocurrencies that misconfigured the way it parsed transactions over two years ago.

The following takes place in a single transaction:

1. Contract 1 sends funds to some number of Coinbase addresses
2. Contract 1 makes a call to another contract, which always reverts.

Coinbase didn't recognize the revert, meaning the on-chain balance stayed the same but Coinbase credited the deposit.



Source: Coinbase Bug Allowed Users To Steal Unlimited ETH, Wallet Paid $10K Bounty For Discovery

Disclaimer: all opinions are my own, not representing Coinbase here

QUADRIGACX

JANUARY 14, 2019

- **QuadrigaCX founder and CEO Gerald Cotten death announced**
  - Announced by his widow, Jennifer Robertson, that he “died due to complications with Crohn’s disease on December 9, 2018, while traveling in India, where he was opening an orphanage in India … for children in need”
- Link shared by QuadrigaCX Twitter account: https://www.quadrigacx.com/gerald-cotten (no longer functional link as of 4/11/19)

Sources: https://www.coindesk.com/quadriga-creditor-protection-filing
https://www.chepicap.com/en/news/7210/the-quadrigacx-timeline-as-it-happened.html

AUTHOR: NADIR AKHTAR

QUADRIGACX

JANUARY 16, 2019

- **User complains about long Bitcoin withdrawal time**
  - Taking over 24h for withdrawal
  - Twitter account attributes delays to “higher demand for crypto” and that “wallets are constantly being refilled”

Sources: https://www.coindesk.com/quadriga-creditor-protection-filing
https://www.chepicap.com/en/news/7210/the-quadrigacx-timeline-as-it-happened.html

AUTHOR: NADIR AKHTAR

QUADRIGACX

JANUARY 29, 2019

- **Exchange goes offline without prior announcement**
  - Website stated “unannounced system maintenance upgrades” as reason for being offline
  - Reddit users start suspecting exit scam

Sources: https://www.coindesk.com/quadriga-creditor-protection-filing
https://www.chepicap.com/en/news/7210/the-quadrigacx-timeline-as-it-happened.html

AUTHOR: NADIR AKHTAR

QUADRIGACX

JANUARY 31, 2019

Some background:

- **Roughly 115,000 users**
- $70 million CAD in fiat owed
- $180 million CAD in crypto owed
- Unknown what amount rested in cold wallet – only alleged that hot wallet contained “minimal amount of coins”
  - If not actively using coins, good to move to offline (cold) wallet to prevent theft

Sources: https://www.coindesk.com/quadriga-creditor-protection-filing
https://www.chepicap.com/en/news/7210/the-quadrigacx-timeline-as-it-happened.html

AUTHOR: NADIR AKHTAR

QUADRIGACX

JANUARY 31, 2019

- **Quadriga files for creditor protection**
  - Quadriga's site goes blank aside from statement confirming bankruptcy proceedings begun, along with affidavit showing exchange filed for consumer protection
  - Robertson alleged, "After Gerry's death, Quadriga's inventory of cryptocurrency has become unavailable and some of it may be lost."
  - Cotten held "sole responsibility for handling funds and coins" according to Robertson
    - "Cotten was the custodian of 26,500 Bitcoin, 11,000 Bitcoin Cash, 11,000 Bitcoin Cash SV, 25,000 Bitcoin Gold, around 430,000 ETH, and roughly 200,000 Litecoin. After Cotten's death, access to these funds allegedly became impossible as knowledge of where the private keys are died with Cotten. **The exchange owes its customers $190 million.**"

Sources: https://www.coindesk.com/quadriga-creditor-protection-filing https://www.chepicap.com/en/news/7210/the-quadrigacx-timeline-as-it-happened.html

AUTHOR: NADIR AKHTAR

QUADRIGACX

FEBRUARY 3, 2019

- **Twitter users start investigating Quadriga themselves**
  - Kraken CEO Jesse Powell (@ProofofResearch) instigated first investigation into Quadriga's transaction history using crowdsourced data, leading to a discovery of an interesting connection or coincidence between Quadriga and Mt. Gox. It turned out that some addresses connected to Mt. Gox may have been sending funds to a wallet associated with several Quadriga transactions.
    - There were reports of large liquidations from the trustee of the exchange, Nobuaki Kobayashi, liquidated tens of thousands of Bitcoin and Bitcoin Cash last year. Possible for Quadriga to have bought it coincidentally.
    - Point is, there's no conclusive evidence of any connection between the two – just chance.
  - Discovered while going down this rabbit hole was that outgoing transactions have been made since Cotten's alleged passing, meaning that **Quadriga never really lost ahold of their access to these funds.**

Sources: https://www.coindesk.com/quadriga-creditor-protection-filing https://www.chepicap.com/en/news/7210/the-quadrigacx-timeline-as-it-happened.html

AUTHOR: NADIR AKHTAR

QUADRIGACX

FEBRUARY 4, 2019

- **Petition for Kraken to buy out Quadriga**
  - A petition began on Change.org for Kraken to buy out Quadriga as a way to “honor it’s [sic] users [sic] funds and to take control of the Quadriga exchange”
  - Currently has 31 out of 100 as of 4/11/19

Sources: https://www.coindesk.com/quadriga-creditor-protection-filing
https://www.chepicap.com/en/news/7210/the-quadrigacx-timeline-as-it-happened.html

AUTHOR: NADIR AKHTAR

QUADRIGACX

FEBRUARY 5, 2019

- **Quadriga co-founder used *fake name***
  - Quadriga co-founder Michael Patryn isn't who he claims to be – his real name is Omar Dhanani, a "convicted criminal charged with fraud for his role in operating an online marketplace for identity theft"
  - Unsure where he is now

Sources: https://www.coindesk.com/quadriga-creditor-protection-filing
https://www.chepicap.com/en/news/7210/the-quadrigacx-timeline-as-it-happened.html

AUTHOR: NADIR AKHTAR

QUADRIGACX

FEBRUARY 5, 2019

- **Quadriga co-founder used *fake name***
  - Quadriga co-founder Michael Patryn isn't who he claims to be – his real name is Omar Dhanani, a "convicted criminal charged with fraud for his role in operating an online marketplace for identity theft"
  - Unsure where he is now
- Quadriga given time to attempt to restructure financial situation to avoid bankruptcy

Sources: https://www.coindesk.com/quadriga-creditor-protection-filing
https://www.chepicap.com/en/news/7210/the-quadrigacx-timeline-as-it-happened.html

AUTHOR: NADIR AKHTAR

QUADRIGACX

FEBRUARY 6, 2019

- **Gerald Cotten's official death certificate discovered**
  - Death date December 9, 2018, corresponding to widow Robertson's attestation
  - Looks like he either didn't fake his death, or he did so very well

Sources: https://www.coindesk.com/quadriga-creditor-protection-filing
https://www.chepicap.com/en/news/7210/the-quadrigacx-timeline-as-it-happened.html

5 CAPTURE THE ETHER!