Next Steps with Blockchain Technology

Eliezer Kanal & Gabriel Somlo
Previous models of computing

Data Storage: Database

Program Execution: Local
Blockchain

**Data Storage:**
Blockchain or Network

**Program Execution:**
Network
Next Steps with Blockchain Technology

Hash: 45af...
Prev: 39e1...
Txn
Txn
Txn
Txn

Hash: 39e1...
Prev: 90f9...
Txn
Txn
Txn
Txn

Hash: 90f9...
Prev: a1c4...
Txn
Txn
Txn
Txn

Hash: a1c4...
Prev: 5668...
Txn
Txn
Txn
Txn

Time
Hash: 45af...
Prev: 39e1...

Hash: 39e1...
Prev: 90f9...

Hash: 90f9...
Prev: a1c4...

Hash: a1c4...
Prev: 5668...

Time
<table>
<thead>
<tr>
<th>Candidate</th>
<th>Votes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob</td>
<td>0</td>
</tr>
<tr>
<td>Jim</td>
<td>0</td>
</tr>
<tr>
<td>Frank</td>
<td>0</td>
</tr>
</tbody>
</table>

State: 1
State: 1

<table>
<thead>
<tr>
<th>Candidate</th>
<th>Votes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob</td>
<td>0</td>
</tr>
<tr>
<td>Jim</td>
<td>0</td>
</tr>
<tr>
<td>Frank</td>
<td>0</td>
</tr>
</tbody>
</table>

Bob: 1 vote
Frank: 1 vote
<table>
<thead>
<tr>
<th>Candidate</th>
<th>Votes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob</td>
<td>1</td>
</tr>
<tr>
<td>Jim</td>
<td>0</td>
</tr>
<tr>
<td>Frank</td>
<td>1</td>
</tr>
</tbody>
</table>

State: 2
State: 1

<table>
<thead>
<tr>
<th>Candidate</th>
<th>Votes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob</td>
<td>0</td>
</tr>
<tr>
<td>Jim</td>
<td>0</td>
</tr>
<tr>
<td>Frank</td>
<td>0</td>
</tr>
</tbody>
</table>

State: 2

<table>
<thead>
<tr>
<th>Candidate</th>
<th>Votes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob</td>
<td>1</td>
</tr>
<tr>
<td>Jim</td>
<td>0</td>
</tr>
<tr>
<td>Frank</td>
<td>1</td>
</tr>
</tbody>
</table>
Equivalent to:

State: 1

<table>
<thead>
<tr>
<th>Candidate</th>
<th>Votes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob</td>
<td>0</td>
</tr>
<tr>
<td>Jim</td>
<td>0</td>
</tr>
<tr>
<td>Frank</td>
<td>0</td>
</tr>
</tbody>
</table>

State: 2

State 1 plus...

- Bob: 1 vote
- Frank: 1 vote
Blockchain: Executive Summary

**Pros:**
- Authentication built-in
- Easy to audit history
- Easy to detect data manipulation
- Very difficult to disrupt

**Cons:**
- Proof-of-work very inefficient
- State updates are slow
- Best for simple computations
# Bitcoin: Mining

## Input
- Previous block signature
- Bunch of transactions
- Random number

## Signature Transactions Random # Output

<table>
<thead>
<tr>
<th>Signature</th>
<th>Transactions</th>
<th>Random #</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>482AA...</td>
<td>txn 1, 17, 88, 452</td>
<td>1</td>
<td>854A3...</td>
</tr>
<tr>
<td>482AA...</td>
<td>txn 1, 17, 88, 452</td>
<td>2</td>
<td>B4221...</td>
</tr>
<tr>
<td>482AA...</td>
<td>txn 1, 17, 88, 452</td>
<td>3</td>
<td>0249F...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Block #509169

**Summary**

<table>
<thead>
<tr>
<th>Number Of Transactions</th>
<th>1915</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output Total</td>
<td>10,289.28130284 BTC</td>
</tr>
<tr>
<td>Estimated Transaction Volume</td>
<td>1,818,669,254.05 BTC</td>
</tr>
<tr>
<td>Transaction Fees</td>
<td>0.4883376 BTC</td>
</tr>
</tbody>
</table>

**Height**

- 509169 (Main Chain)

**Timestamp**

- 2018-02-14 15:16:59

**Received Time**

- 2018-02-14 15:16:59

**Relayed By**

- 58COIN

**Difficulty**

- 2,874,874,234,415.94

**Bits**

- 3922928656

**Size**

- 1132,416 bytes

**Weight**

- 3992.574 kWU

**Version**

- 0x20000000

**Nonce**

- 1858880081

**Block Reward**

- 12.5 BTC

**Transactions**

<table>
<thead>
<tr>
<th>Hash</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>14DT5uaUlb77cwR8BuNJ1n6WBIhZY6FEnIg6gLs</td>
<td>12.0803378 BTC</td>
</tr>
<tr>
<td>0 BTC</td>
<td></td>
</tr>
</tbody>
</table>

0 Inputs (Newly Generated Coins)

Unable to decode output address

<table>
<thead>
<tr>
<th>Hash</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>14DT5uaUlb77cwR8BuNJ1n6WBIhZY6FEnIg6gLs</td>
<td>12.9853378 BTC</td>
</tr>
<tr>
<td>12.0803378 BTC</td>
<td>0 BTC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hash</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>14DT5uaUlb77cwR8BuNJ1n6WBIhZY6FEnIg6gLs</td>
<td>0.4983378 BTC</td>
</tr>
<tr>
<td>0.4983378 BTC</td>
<td>0.1493378 BTC</td>
</tr>
<tr>
<td>5.0163378 BTC</td>
<td>5.0163378 BTC</td>
</tr>
</tbody>
</table>
```
[root@DeltaUser1 DeltaUser1.conf]# btccli getwalletinfo
{
   "walletversion": 138000,
   "balance": 14.82300000,
   "unconfirmed_balance": 0.00000000,
   "immature_balance": 0.00000000,
   "txcount": 1,
   "keypoololdest": 1535483250,
   "keypoolsize": 100,
   "paytxfee": 0.00000000,
   "hdmasterkeyid": "722820f65abc8c218892c66c6a5532a45f389b08"
}
[root@DeltaUser1 DeltaUser1.conf]#
```

```
[root@btc-1 btc-1.terra.com.conf]# btccli sendtoaddress mzLLFxpnJJa5L38QMUMzwXanb6suWayCMN 14.823
4aad741923b21bf64a16f664c637f7be6a3b81ca65719dd41bf80668230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
```
[root@DeltaUser1 DeltaUser1.conf]# gettx () {
  > local TXID=${1}
  > btccli decoderawtransaction '${btcl getrawtransaction $TXID}'
}

[root@DeltaUser1 DeltaUser1.conf]#
Koinbase, Inc is a financial institution registered in the U.S. One of the services it offers is to exchange customers' Bitcoin for U.S. Dollars. Customers send BTC to Koinbase's public address:

Koinbase "mtDqnenHsTy1grsnoDscdnurbX598Nzf\n
In return, Koinbase deposits an amount of USD matching the current exchange rate into the each customer's Koinbase checking account.

Four customers sent approximately BTC 50.00 each to Koinbase's public address today (name and BTC address listed below):

Alice "mk8PhnCTpq5NK3C7bMg65Dg4GCY2XJNp6Z"
Bob  "mrd57X42S60Hkm3ca1PV56u1yqLtjEVU61"
Charlie "mxmhKxRhmzTDUPY58Ydantp70zX7VYrWn"
Diane "mne3hNXYhtetpzbh6CJzvJx5TsJawtmpV"

Koinbase monitors a blacklist of reported illegal transactions, and is required to flag and refer suspicious transactions to law enforcement for further investigation. The list of known illegal transactions currently contains one instance of a ransomware attack being paid off, in the amount of BTC 100.00. That transaction's TxID (hash) is:

014dd5ff639fbaed2e23f94d6d73e5bb4bc0cc45bafc8f88bf6b25a5023122c8

As Koinbase's security analyst, you are tasked with determining which, if any, of these four customers' transactions to flag as potentially suspicious.
Tracing Transaction History
Tracing Transaction History
Blockchain programming is hard!

- Over $40M were stolen from TheDAO due to a bug in the implementation (June 2016)
- $32M were stolen due to a bug in a commonly used contract (June 2017)
- Bugs in smart contracts cannot be fixed after deployment

We want to build correct software, but current approaches have been shown to have security vulnerabilities
Obsidian: a new programming language

- Obsidian is a blockchain-based language with the goal of minimizing the risk of common security vulnerabilities
- Obsidian contains core features to allow users to write safe programs easily and effectively
- Obsidian programs consist of **contracts**, which contain fields, states, and **transactions**
Obsidian: a new programming language

Goals

• Make certain vulnerabilities impossible
• Make it easier to write correct programs
• Show effectiveness and correctness

Components

1. Typestate-oriented programming
2. Resource types
Typestate

• Blockchain programs commonly state-oriented
• Obsidian makes state first-class
  - An object in Obsidian has a state that restricts which transactions can be invoked on it.
• State transitions can change the state of an object
Typestate

```solidity
contract LibraryPatron {
    state NoCard {
        transaction getCARD() {
            ...
            -> HasCard;
        }
    }

    state HasCard {
        transaction getBook() {
            ...
        }
    }
}
```

• A **LibraryPatron** is always in either the **NoCard** or **HasCard** state
Typestate

```solidity
contract LibraryPatron {
    state NoCard {
        transaction getCard() {
            ...
            -> HasCard;
        }
    }

    state HasCard {
        transaction getBook() {
            ...
        }
    }
}
```

- A `LibraryPatron` is always in either the `NoCard` or `HasCard` state.

- `getBook` can only be called in `HasCard`; calling from `NoCard` state results in compile-time error.
Typestate

```solidity
contract LibraryPatron {
    state NoCard {
        transaction getCard() {
            ...
            -> HasCard;
        }
    }

    state HasCard {
        transaction getBook() {
            ...
        }
    }
}
```

- **A LibraryPatron is always in either the NoCard or HasCard state.**
- **getBook can only be called in HasCard; calling from NoCard state results in compile-time error**
- **→HasCard is a state transition**
Typestate – Other common applications

Voting

• Not Eligible
• Eligible, not voted
• Eligible, voted
Typestate – Other common applications

Supply chain

• Browsing
• Purchasing
• Order in processing
• Shipping
• Delivering to customer
• Return requested
• Delivering to business
• Returned
Typestate – Other common applications

Supply chain
• Browsing
• Purchasing
• Order in processing
• Shipping
• Delivering to customer
• Return requested
• Delivering to business
• Returned

Customer management
Manufacturing
Add steps for wholesale distributor
Linear Types

• Blockchain programs often manage some kind of resource
  - e.g., cryptocurrency, votes, items in supply chain
• **Linear types** allow the compiler to enforce “resource safety”:
  - Resources cannot be used more than once
  - Resources must be used before leaving the current scope (i.e., don’t lose it)
Linear Types

```solidity
resource contract Money {...};

contract Account {
    Money balance;

    transaction closeAccount(Account a) {
        a.withdraw(balance);
        balance = new Money(0);
    }

    transaction withdraw(Money m) {...}
}
```

- Financial application example
- `balance` is a type of `Money`, which is a linear type
Linear Types

resource contract Money {...};

contract Account {
    Money balance;

    transaction closeAccount(Account a) {
        a.withdraw(balance);
        balance = new Money(0);
    }

    transaction withdraw(Money m) {...}
}

- When balance is moved out of scope, we need to create a new Money object to replace it
- The new Money is created with a value of 0
- Note that we’re not referring to the actual amount of money, we’re referring to the code used to track the money
- Code security, not accounting
Linear Types

```solidity
resource contract Money {...};

contract Account {
    Money balance;

    transaction closeAccount(Account a) {
        a.withdraw(balance);
        a.withdraw(balance);
        balance = new Money(0);
    }

    transaction withdraw(Money m) {...}
}
```

- Introducing bug… spending more `Money` than available
- Program would fail when trying to compile, rather than when the user tried to run the program
Usability

Programmers should be able to write correct Obsidian code easily and effectively. Creating an intuitive language is hard! Many difficult design choices exist
Which is “correct”?
Usability study

Participants were given a description of a voter registration system for a hypothetical democratic nation.
Usability study

1. Write pseudocode to implement program.
2. Given a state diagram modeling the voter registration system, modify pseudocode.
3. Given Obsidian tutorial (with no information on state transitions) invent syntax for state transitions and complete an Obsidian contract.
4. Shown three options for state transitions, complete a brief contract for each option.
5. Choose one of the three options and use it to complete the Obsidian program from part 3.
Usability study – Findings

• Programmers do not naturally consider state-based design when architecting code
• Most intuitive design: include all possible state actions explicitly within the state
Summary

Bitcoin simulator
• Virtual implementation of Bitcoin network
• Useful for forensic analysis

Obsidian
• Secure-by-design language for blockchain development
• Typestate and linear resources help users write safe programs easily and effectively
• Usable programming language design requires iteration and user testing
Contact Information

Presenters

Elli Kanal
Technical Manager
Email: ekanal@cert.org

Gabe Somlo
Cybersecurity Researcher
Email: glsomlo@cert.org