

---

# Gambling Contract Detection through Flow Analysis

— Daniel Chang, Zhiyi Huang,  
Yichun Li —

---

# Can we detect gambling contracts?

- Yes



# Data

- Each transaction will consist of a triplet of data:
  - Transaction value
  - Internal transaction value
  - Token transfer value
- 223 contracts gathered
  - 72 gambling
  - 151 non-gambling (games, exchanges, social, governance, etc.)
- Each example (row of data) has 100 transactions

Transaction Hash: 0x3cd319f585bcef6c9d88b6edc4f7b5a257533317aff7fed4c131560539505cdc

Status: Success

Block: 9944880 8 Block Confirmations

Timestamp: 1 min ago (Apr-26-2020 12:36:25 AM +UTC)

From: 0xce235362e7d11de16696fed6adad9137f9ad8ada

To: Contract 0xd1ceeeee83f8bcf3bedad437202b6154e9f5405 (Dice2Win)

Value: 1 Ether (\$194.78)

Transaction Fee: 0.00063968 Ether (\$0.12)

Gas Limit: 150,000

Gas Used by Transaction: 79,960 (53.31%)

Gas Price: 0.000000008 Ether (8 Gwei)

Nonce Position 32666 22

Input Data:

Function: placeBet(uint256 betMask, uint256 modulo, uint256 commitLastBlock, uint256 commit, bytes32 r, bytes32 s)

MethodID: 0x5e83b463

```
[0]: 0000000000000000000000000000000000000000000000000000000000000000
[1]: 0000000000000000000000000000000000000000000000000000000000000002
[2]: 0000000000000000000000000000000000000000000000000000000000097bfff5
[3]: a01e485a49198b140df0ec0f99fa36954012cbc30300508e66b3f2630c609b91
[4]: c9186285aed7ca01f87fd669646de6630810c1307927743a73395b1bc1dac0e
[5]: 5838b495a723bf8ae857aeeef4698e31e92b91acf70ce1085148cb4997b5710d
```

View Input As

Decode Input Data

 Are you the contract creator? [Verify and Publish](#) your contract source code today!

[Decompile ByteCode](#)  [Switch to Opcodes View](#) [Similar Contracts](#)

```
0x6080604052600436106102255760003560e01c80636b5c5f391161012357806396bc0dd611610ab578063d56b28891161006f578063d56b28891461097f578063e5ef5c8914610994578063f2fde38b146109a9578063f4ae78fc14610
9dc578063f5aff85614610a1b57610225565b806396bc0dd614610851578063a8283c2414610884578063b27505b6146108f8578063b8b3eb021461092b578063c4dd3abe1461095557610225565b80638622cbf1116100f25780638622cb
f11461079757806386767f1a146107c35780638da5cb5b146107d85780638f32d59b146107ed578063937b9dff1461081657610225565b80636b5c5f39146106e0578063710168a6146106f5578063733a6ae61461072e5780638616233f1
461075e57610225565b806342729c14116101b15780635b06788f116101755780635b06788f146105c25780635e6289d8146105f57806364eb147a1461062e578063683d04d51461067557806368c18745146106a757610225565b806342
729c14146104ba5780634e27b907146104cf5780634e46a9b3146105085780634eeb716b146105325780635a5d7e0e146105ad57610225565b80633451664c116101f85780633451664c146103525780633df4b9f9146103915780633f823
ef5146103a657806340a53329146103df578063426b11d01461042457610225565b8063054f38fc1461022a578063171515ba1461027f57806318cb067f146102d65780631953b3cf14610313575b600080fd5b34801561023657600080fd
5b506102636004803603604081101561024d57600080fd5b506001600160a01b038135169060200135610a52565b604080516001600160a01b039092168252519081900360200190f35b34801561028b57600080fd5b506102b8600480360
360408110156102a257600080fd5b506001600160a01b038135169060200135610aa2565b60408051938452602084019290925282820152519081900360600190f35b3480156102e257600080fd5b50610311600480360360408110156102
f957600080fd5b506001600160a01b03813516906020013515610b2e565b005b34801561031f57600080fd5b506103116004803603606081101561033657600080fd5b506001600160a01b038135169060208101359060400135610ba05
65b34801561035e57600080fd5b50610311600480360360608110156103757600080fd5b506001600160a01b038135169060208101359060400135610c53565b34801561039d57600080fd5b50610263610ce9565b3480156103b2576000
80fd5b50610263600480360360408110156103c957600080fd5b506001600160a01b038135169060200135610cf8565b3480156103eb57600080fd5b506104126004803603602081101561040257600080fd5b50356001600160a01b03166
10d6f565b60408051918252519081900360200190f35b610311600480360360c081101561043a57600080fd5b6001600160a01b0382358116926020810135926040820135909216916060820135919081019060a081016080820135640100
00000081111561047b57600080fd5b8201836020820111561048d57600080fd5b80359060200191846001830284011164010000000083111756104af57600080fd5b919350915035610d8a565b3480156104c657600080fd5b506104126
10a7a565b3480156104df57600080fd5b50610412600480360360408110156104f757600080fd5b506001600160a01b038135169060200135610a7a565b34801561051057600080fd5b5061052b57600080
```

Transaction Hash: 0x980a34d98929533511cd55494d0f2df9c6204a52f838340d8293b2316225bc14

Status: Success

Block: 9944864 43 Block Confirmations

Timestamp: 8 mins ago (Apr-26-2020 12:32:42 AM +UTC)

From: 0x00000000c0293c8ca34dac9bcc0f953532d34e4d







To: Contract 0xd1ceeeee83f8bcf3bedad437202b6154e9f5405 (Dice2Win) ✓  
L TRANSFER 0.592 Ether from Dice2Win To → 0xd61677f8cd372901c01...

Value: 0 Ether (\$0.00)

Transaction Fee: 0.000236978 Ether (\$0.05)

[Click to see More](#) ↓

Private Note: To access the Private Note feature, you must be [Logged In](#)

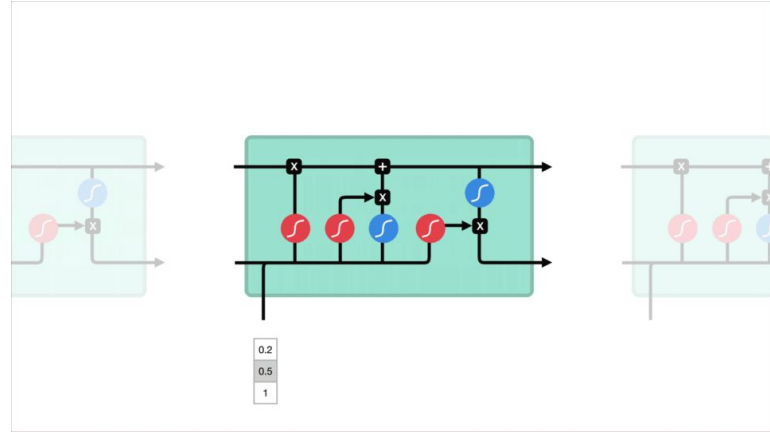
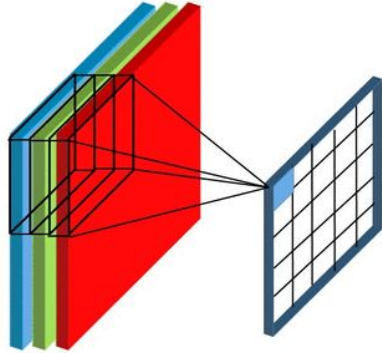
Transaction Hash:	0xa9ab52d7e1ad9665b2c86b263255c870f0a5897e5a4c35c4d648cac3f0cd5710 
Status:	 Success
Block:	9686819 <span>258101 Block Confirmations</span>
Timestamp:	39 days 20 hrs ago (Mar-17-2020 04:05:24 AM +UTC)
From:	0x3308e8f559631f677aacfc6a5d154b285ddd935c 
To:	Contract 0xc12d1c73ee7dc3615ba4e37e4abfdbddfa38907e (KickICO Token)  
Tokens Transferred:	From 0x3308e8f559631f6... To KickICO: Old Token 2 For 1,030,000 (\$6.46)  KickToken (KICK)
Value:	0 Ether (\$0.00)
Transaction Fee:	0.00065608873442 Ether (\$0.13)

[Click to see More](#) 

Private Note: To access the Private Note feature, you must be [Logged In](#)

# Model

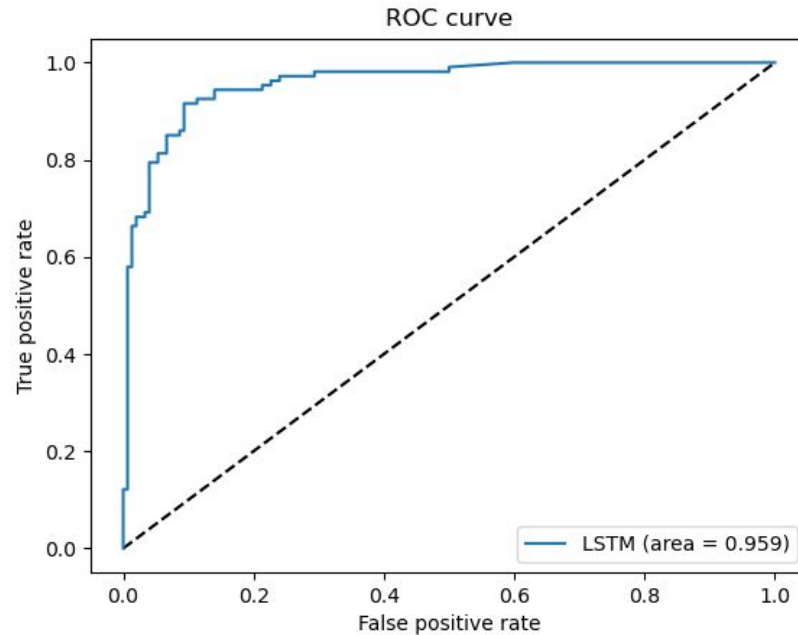
- 1 One-dimensional Convolutional Neural Network (CNN) layer
- 2 Bidirectional Long Short-term Memory (Bi-LSTM) layers
- 1 Output layer: gambling (1) or non-gambling (0)





## Result

**90%  $\pm$  5% Accuracy**



# Future work

- More complex model
  - model capable of using longer sequences (transformers)
- More data from more active contracts
- Add other features from the transactions: gas, transaction fees, etc.
- How could a gambling contract fool our model?
  - Spacing out transactions with dud transactions
  - Mimic transaction patterns of other contract

# Question?

<https://github.com/Ortiane/Smart-Contract-Gambling-Detection>