

# HORIZON

## BLOCKCHAIN GAMES



Specialized State Channels for  
Turn-based Multiplayer Blockchain Video Games

Peter Kieltyka — <https://horizontgames.net> — July 2018

# Virtual Items + Blockchain → Crypto Items

- “True Digital Ownership”
- Decentralized — trustless protocol level security for digital goods
- Open economies that are standardized & interoperable
- Cryptographically secure
- Open networks for trading and selling

# Video Games + Blockchain → Decentralized Games

- Utility for crypto virtual items
- Decentralized
  - Byzantine fault tolerant
  - Distributed (peer-to-peer)
  - Economic rewards
  - Trustless
- State resolution native to a blockchain
- Provably-fair gameplay
- Open source, open ecosystem, open economy
  - Modability to infinity, mass collaboration

# Blockchain Games

1



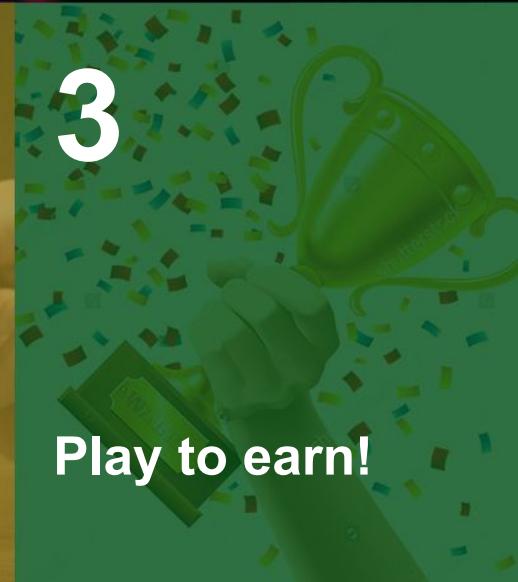
True Digital  
Ownership

2



Provably-Fair  
Gameplay

3



Play to earn!

...open network, open ecosystem and open source



# SkyWeaver

Fast-paced strategy trading card game, on the blockchain



# CONGRATULATIONS

You just won a new card!



Add to my collection

# Decentralized Video Game Design Goals

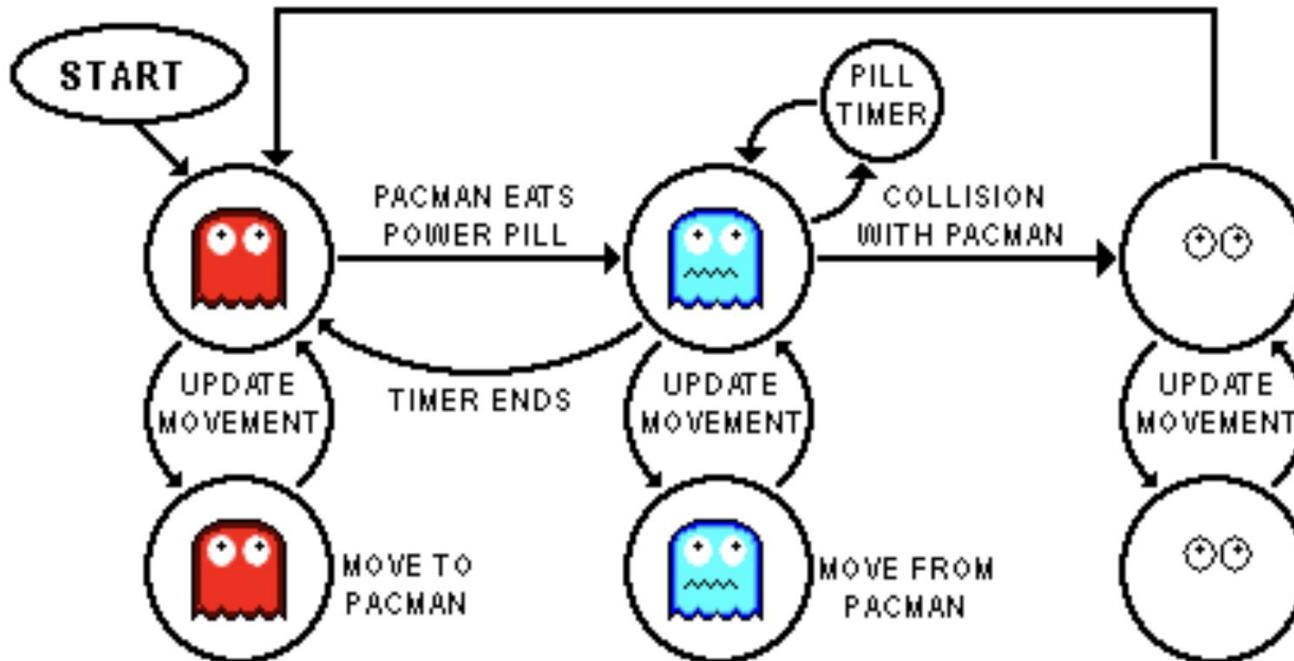
1. High-fidelity, real-time, fast! Just like a normal video game
2. Provable game victory or fraud
3. Low-cost to operate on blockchain infrastructure
4. Open source game server and client

# Naive Blockchain Game

- On-chain game logic, and each move as an on-chain transaction
  - Constrained by distributed systems laws of physics (15 tx/sec)
  - Slow finality (2 to 10 minutes)
  - Expensive
  - Unnecessarily saving too much state to a blockchain
- Hint: not going to work!

# State + UI

# Finite-State Machines



# State Channels

- Off-chain signed state updates between multi-parties using a deterministic state machine symmetrically on-chain
- On-chain deposits + trivial fraud proofs keep everyone honest
- Common uses: payment channels
- Some great research teams + projects:
  - Counterfactual Generalized State Channels by L4
  - Celer Networks Generalized State Channels
  - Perun Virtual Channels
  - Funfair Fate Channels
  - Raiden
  - .. + others

# Specialized State Channels

- Real-time turn-based multiplayer video games
- Deposit is held as a security deposit / collateral
  - Ether is not exchanged between individuals
- Off-chain game-play that is deterministic + provable as single terminal state
- Virtual hub to act as intermediary instead of routing state between parties
  - State availability
  - State relay
  - State proofing
  - ..other



a platform for decentralized & open source  
video games on Ethereum

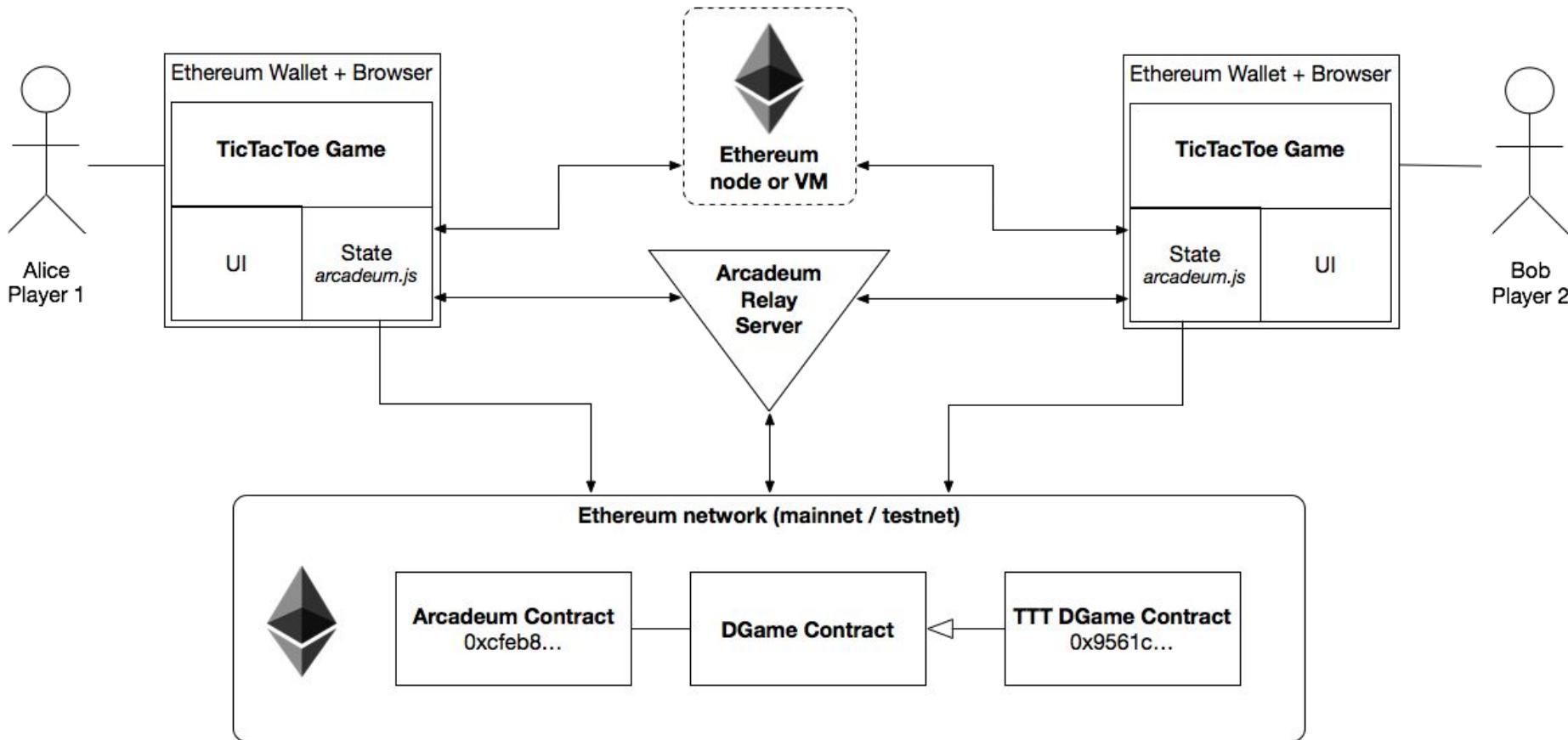
<https://arcadeum.net>



# Arcadeum Stack

- `Arcadeum.sol` — arcade hub contract players
  - Deposit / withdraw security collateral (aka open / close channel)
  - Victory proofing, cheater proofing
- `DGame.sol` — FSM base game library for game state + logic
- `arcadeum.js` — JavaScript client library for Arcadeum and DGame apps
  - Client-side state management library (think: Redux store / reducers)
  - Ethereum contract interfacing (via ethers.js)
  - Ephemeral key generation and exchange
  - Commit / reveal interaction for two-party RNG
  - Victory or fraud proofing
- Arcadeum Server — Go server for relaying state + availability
  - Staked + bound by laws of Arcadeum contract

# Arcadeum Topology



```
contract DGame {
```

```
    function initialState(bytes publicSeed0, bytes publicSeed1) public pure  
        returns (MetaState);
```

```
    function winnerImplementation(State state) internal pure  
        returns (Winner);
```

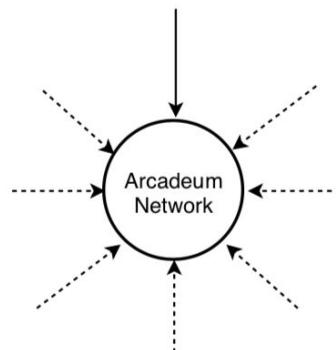
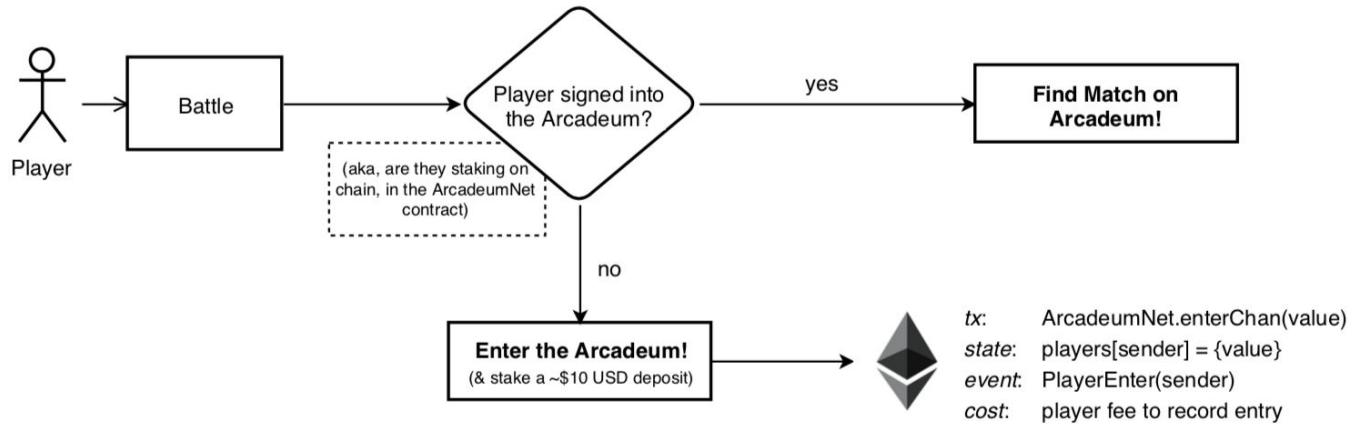
```
    function nextPlayersImplementation(State state) internal pure  
        returns (NextPlayers);
```

```
    function isMoveLegalImplementation(State state, Move move) internal pure  
        returns (bool, int32);
```

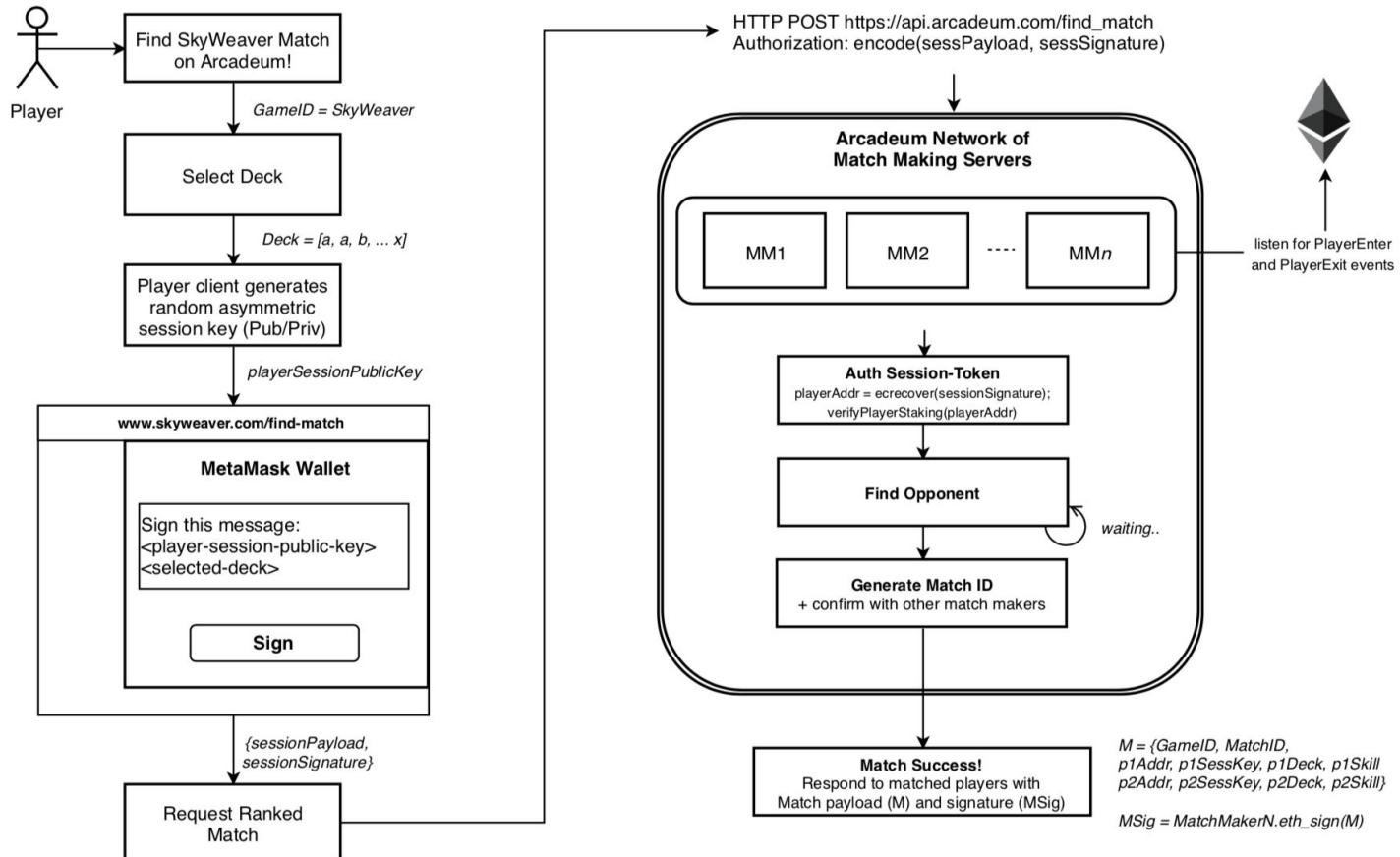
```
    function nextStateImplementation(State state, Move move) internal pure  
        returns (MetaState);
```

```
}
```

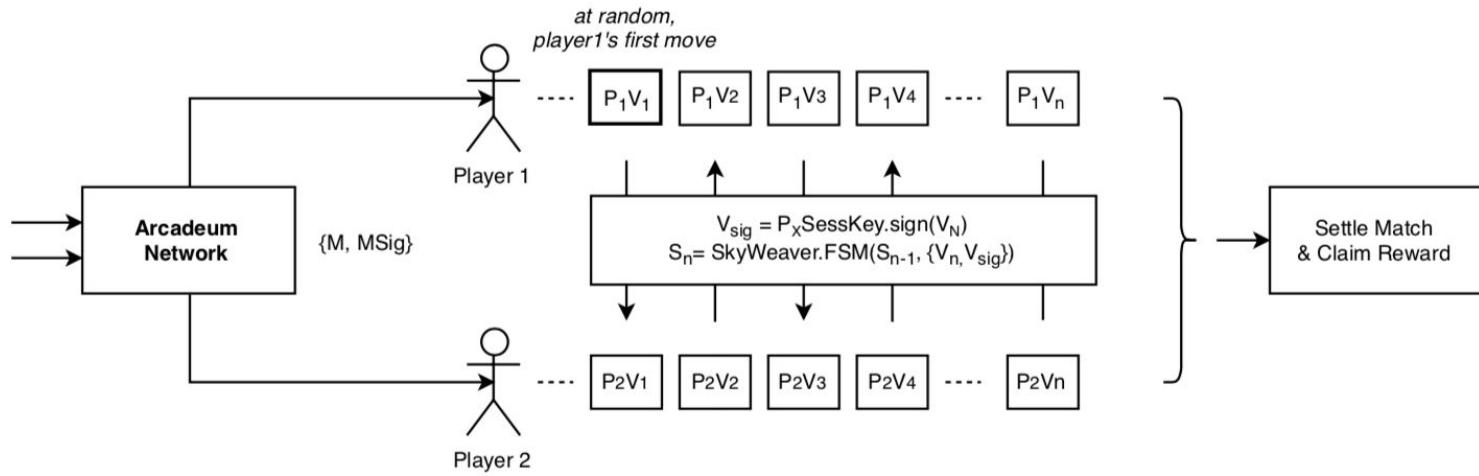
## Arcadeum: Player Battle Initialization



# Arcadeum: Player Match Making



# Arcadeum: Off-Chain Game Play



$M = \{GameID, MatchID,$   
 $p1Addr, p1SessKey, p1Deck, p1Skill$   
 $p2Addr, p2SessKey, p2Deck, p2Skill\}$

$MSig = \text{MatchMakerN.eth\_sign}(M)$

Open sourced!!



[/horizon-games/arcadeum](https://github.com/horizon-games/arcadeum)



1. peter@pak.local | ~/Dev/go/src/github.com/horizon-games/arcadeum (node)

```
x node
eth_getFilterChanges
eth_getTransactionReceipt
eth_getCode
eth_uninstallFilter
eth_sendTransaction

Transaction: 0xfaa6f7eea3668ad16405f741229194e8d3a328b5e419e90a2df30898b285f846
Gas usage: 27008
Block Number: 8
Block Time: Wed Jul 25 2018 07:54:50 GMT+0800 (Hong Kong Standard Time)

eth_getTransactionReceipt
eth_getBlockByNumber
eth_getBlockByNumber
```

Shell

```
test -f ./etc/arcadeum-server.conf || sed -e \
's|!working_dir| = """$!working_dir = "/Users/peter/Dev/go/src/github.com/horizon-games/arcadeum/server/"|' \
./etc/arcadeum-server.conf.sample > ./etc/arcadeum-server.conf
$ sh -c GOGC=off go build -i -o ./bin/arcadeum-server ./cmd/arcadeum-server/main.go && ./bin/arcadeum-server -config=etc/arcadeum-server.conf
2018/07/25 07:54:20 ARCADEUM Server started :8000; connect at /ws
```

zsh

```
Deploying Migrations...
... 0xa5608982562ed8c9a11178125853d9b62e45e580e29508e198a1a910e7379141
Migrations: 0xe7800f7e598cc8b0bb87894b0f60dd2a88d6a8ab
Saving successful migration to network...
... 0xf3d813ac454cc6356802bbacb99ee71cf1d7b5e4877f46ac2df4f64060a0427f
Saving artifacts...
Running migration: 2_deploy_arcadeum.js
Deploying Arcadeum...
... 0xf5eedd2ce42a65028d02c65648e082bb02a8938a2b0bb612c15233720825b1614
Arcadeum: 0xfcbe869f69431e42cdb54a4f4f105c19c080a601
Saving successful migration to network...
... 0xc254e4b1981d8c1644e4c26a8d1d51978745b6b2f80c899bcd89562f0e045190
Saving artifacts...
⚡ Done in 4.71s.
[peter@pak ~/Dev/go/src/github.com/horizon-games/arcadeum]$ 
```

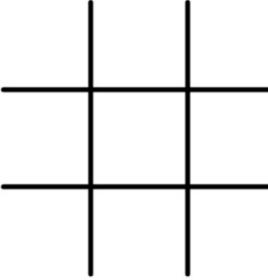
zsh

```
Deploying Migrations...
... 0x0d8c39a82dde93a8478144e80c2a720f230a0497affdf180e7538da0b1915e02
Migrations: 0xc89ce4735882c9f0f0fe26686c53074e09b0d550
Saving successful migration to network...
... 0x6fa8fd639b74dce668fdb0b7d1f9c09875429d9677ab37b48f343af02eae99e
Saving artifacts...
Running migration: 2_deploy_ttt.js
Deploying TTT...
... 0x5614ff1adaaaaae4356016e7c94640e79ac3e2d5dd72c0b7eaff891fccadf5e
TTT: 0x9561c133dd8580860b6b7e504bc5aa500f0f06a7
Saving successful migration to network...
... 0xfaa6f7eea3668ad16405f741229194e8d3a328b5e419e90a2df30898b285f846
Saving artifacts...
⚡ Done in 4.56s.
[peter@pak ~/Dev/go/src/github.com/horizon-games/arcadeum/examples/ttt]$ 
```

TTT

localhost:3000

- balance:  
0
- current time:  
7/21/2018, 7:54:15 PM
- withdrawal time:  
12/31/1969, 7:00:00 PM
- [deposit](#)
- [start withdrawal](#)
- [finish withdrawal](#)
- [create match](#)



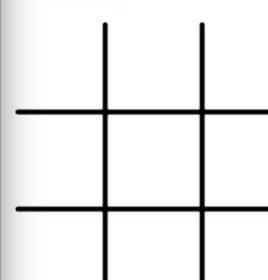
Inspector   Console   Debugger   Style Editor   Shader Editor   Canvas   Performance   ...

Filter output

TTT

localhost:3000

- balance:  
0
- current time:  
7/21/2018, 7:54:15 PM
- withdrawal time:  
12/31/1969, 7:00:00 PM
- [deposit](#)
- [start withdrawal](#)
- [finish withdrawal](#)
- [create match](#)



Elements   Console   Audits   Sources   Network   Performance   Memory   Application   Security   Redux

top | Filter

Default levels ▾   Group similar

TTT

moz-extension://f0308250-38c9-6144-a26a...

localhost 8545

## Confirm

Please review your transaction.

From: test  
...09f0

To: New Recipient  
...a601

Gas Fee: 0.00006501 ETH  
\$0.03 USD

Total: \$461.17 USD

CANCEL CONFIRM

TTT

localhost 8545

TTT

localhost:3000

balance: 0

current time: 7/21/2018, 7:54:26 PM

withdrawal time: 12/31/1969, 7:00:00 PM

- deposit
- start withdrawal
- finish withdrawal
- create match

Console

Elements

Audits

Sources

Network

Performance

Memory

Application

Security

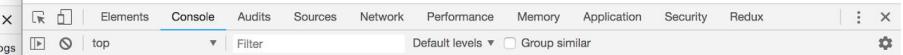
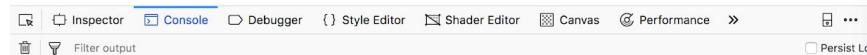
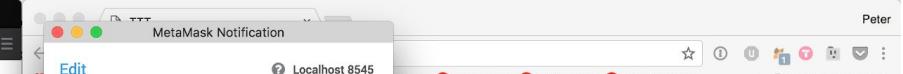
Redux

top

Filter

Default levels

Group similar



The screenshot shows a web browser window with the URL `localhost:3000/#`. The page content is as follows:

- balance:  
10000000000000000000
- current time:  
7/21/2018, 7:54:50 PM
- withdrawal time:  
12/31/1969, 7:00:00 PM

[deposit](#)  
[start withdrawal](#)  
[finish withdrawal](#)  
[create match](#)

A large black tic-tac-toe grid is centered on the page.

At the bottom of the browser window, the following tabs and icons are visible:

- Inspector
- Console
- Debugger
- Style Editor
- Shader Editor
- Canvas
- Performance
- ...
- Persist Log

The screenshot shows a web browser window with the URL `localhost:3000/#`. The page displays a Ethereum wallet interface and a tic-tac-toe board.

**Ethereum Wallet Interface:**

- Header: Private Network
- Account: Account 3 (Address: 0x22...e32b)
- Balances: 999999998.995 ETH (\$461,299,999,536.70)
- Buttons: DEPOSIT, SEND
- Transactions: July 21 2018 19:54, 1 ETH (461.3 USD) - Confirmed

**Tic-Tac-Toe Board:**

A simple 3x3 grid for playing tic-tac-toe.

TTT

moz-extension://f0308250-38c9-6144-a26a...

Signature Request

Account: test

Balance: 999999998.999957 ETH

Your signature is being requested

You are signing:

Message:

Sign to play! This won't cost anything. Player: 0x5cd6cea308b30d0ab38315db7be3a2db2ff253a7

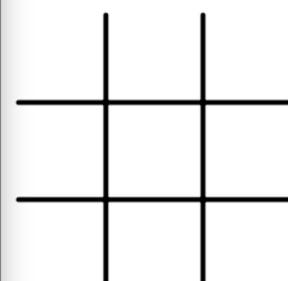
CANCEL SIGN

TTT

localhost:3000/#

Peter

- balance: 10000000000000000000
- current time: 7/21/2018, 7:55:05 PM
- withdrawal time: 12/31/1969, 7:00:00 PM
- deposit
- start withdrawal
- finish withdrawal
- create match



Inspector Console Debugger Style Editor Shader Editor Canvas Performance

Filter output Persist Logs

```
Object { secretSeed: Uint8Array [], arcadeumContract: {}, gameContract: {}, serverAddress: "ws://localhost:8080/", signer: {}, callbacks: (1) [], queue: [], isRunning: true, didQueueChange: false, processedMoves: (2) [], - }
```

Elements Console Audits Sources Network Performance Memory Application Security Redux

top Filter Default levels Group similar

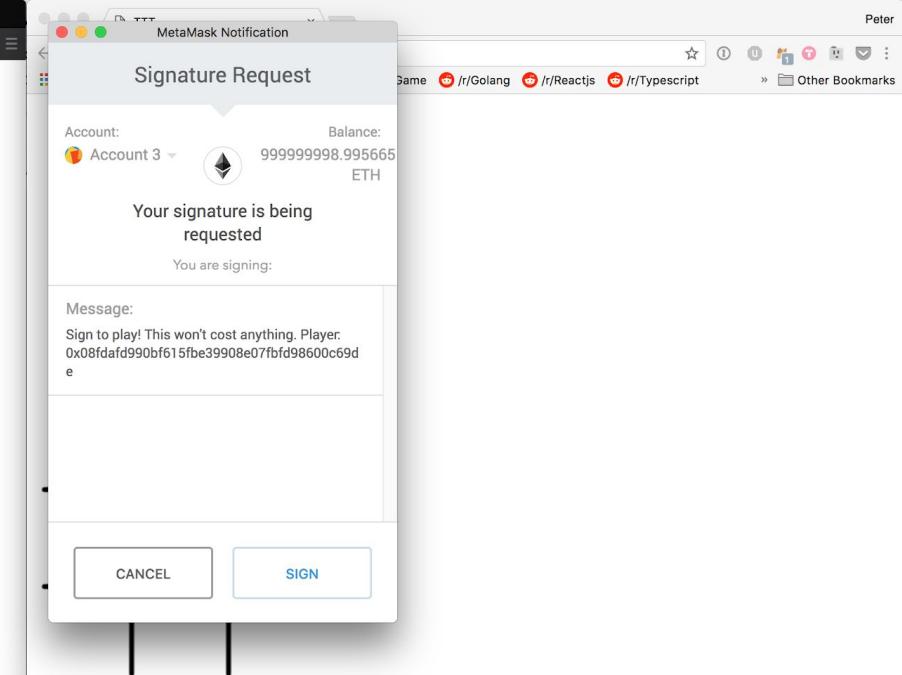
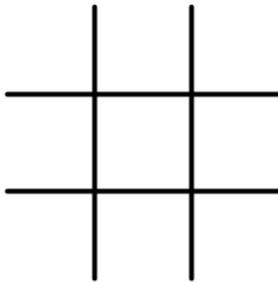
```
>
```

TTT    +

localhost:3000/#

Search

```
• balance:  
1000000000000000000  
  
• current time:  
7/21/2018, 7:55:18 PM  
  
• withdrawal time:  
12/31/1969, 7:00:00 PM  
  
• deposit  
• start withdrawal  
• finish withdrawal  
• create match
```



Inspector Console Debugger Style Editor Shader Editor Canvas Performance

Filter output

```
Object { secretSeed: Uint8Array [], arcadeumContract: {}, gameContract: {}, serverAddress: "ws://localhost:8000/", signer: {}, callbacks: (1) [Object], queue: [], isRunning: true, didQueueChange: false, processedMoves: (2) [Object], ... } index.ts:30:2
```

Elements Console Audits Sources Network Performance Memory Application Security Redux

top Filter Default levels Group similar

```
BasicMatch {secretSeed: Uint8Array(0), arcadeumContract: Contract, gameContract: Contract, serverAddress: "ws://localhost:8000/", signer: JsonRpcsSigner, ... } index.ts:30:2
```

TTT

localhost:3000/#

- balance: 10000000000000000000
- current time: 7/21/2018, 7:55:37 PM
- withdrawal time: 12/31/1969, 7:00:00 PM
- [deposit](#)
- [start withdrawal](#)
- [finish withdrawal](#)
- [create match](#)

Inspector    Console    Debugger    Style Editor    Shader Editor    Canvas    Performance

Console

```

▶ Object { secretSeed: Uint8Array [], arcadeumContract: {}, gameContract: {}, serverAddress: "ws://localhost:8000/", signer: {}, callbacks: (1) [Object], queue: [], isRunning: true, didQueueChange: false, processedMoves: (2) [Object], ... }
undefined
▶ Object { arcadeumContract: {}, gameContract: {}, tag: 0, data: Uint8Array(9), meta: {} }
▶ Object { move: (1) [Object], playerID: 0, data: Uint8Array(1), signature: (1) [Object], stateHash: Uint8Array(32) }
▶ Object { arcadeumContract: {}, gameContract: {}, tag: 1, data: Uint8Array(9), meta: {} }
▶ Object { move: (1) [Object], playerID: 1, data: Uint8Array(1), signature: (1) [Object] }
▶ Object { arcadeumContract: {}, gameContract: {}, tag: 2, data: Uint8Array(9), meta: {} }
▶ Object { move: (1) [Object], playerID: 0, data: Uint8Array(1), signature: (1) [Object], stateHash: Uint8Array(32) }
▶ Object { arcadeumContract: {}, gameContract: {}, tag: 3, data: Uint8Array(9), meta: {} }
▶ Object { move: (1) [Object], playerID: 1, data: Uint8Array(1), signature: (1) [Object] }
▶ Object { arcadeumContract: {}, gameContract: {}, tag: 4, data: Uint8Array(9), meta: {} }

```

TTT

localhost:3000/#

- balance: 10000000000000000000
- current time: 7/21/2018, 7:55:38 PM
- withdrawal time: 12/31/1969, 7:00:00 PM
- [deposit](#)
- [start withdrawal](#)
- [finish withdrawal](#)
- [create match](#)

Console

```

BasicMatch {secretSeed: Uint8Array(0), arcadeumContract: Contract, gameContract: Contract, serverAddress: "ws://localhost:8000/", signer: JsonRpcSigner, ...}
undefined
▶ BasicState {arcadeumContract: Contract, gameContract: Contract, tag: 0, data: Uint8Array(9), meta: {}}
▶ BasicMove {move: (1) [Object], playerID: 0, data: Uint8Array(1), signature: Signature}
▶ BasicState {arcadeumContract: Contract, gameContract: Contract, tag: 1, data: Uint8Array(9), meta: {}}
▶ BasicMove {move: (1) [Object], playerID: 1, data: Uint8Array(1), signature: Signature, stateHash: Uint8Array(32)}
▶ BasicState {arcadeumContract: Contract, gameContract: Contract, tag: 2, data: Uint8Array(9), meta: {}}
▶ BasicMove {move: (1) [Object], playerID: 0, data: Uint8Array(1), signature: Signature}
▶ BasicState {arcadeumContract: Contract, gameContract: Contract, tag: 3, data: Uint8Array(9), meta: {}}
▶ BasicMove {move: (1) [Object], playerID: 1, data: Uint8Array(1), signature: Signature, stateHash: Uint8Array(32)}
▶ BasicState {arcadeumContract: Contract, gameContract: Contract, tag: 4, data: Uint8Array(9), meta: {}}

```

TTT

moz-extension://f0308250-38c9-6144-a26a...

localhost 8545

## Confirm

Please review your transaction.

From: test ...09f0

To: New Recipient ...a601

Gas Fee: 0.00045335 ETH \$0.21 USD

Total: \$0.21 USD

**CANCEL** **CONFIRM**

Object { secretSeed: Uint8Array [], arcadeumContract: {}, gameContract: {}, serverAddress: "ws://localhost:8000/", signer: {}, callbacks: () => [], queue: [], isRunning: true, didQueueChange: false, processedMoves: (2) [ ] }

undefined

Object { arcadeumContract: {}, gameContract: {}, tag: 0, data: Uint8Array(9), meta: {} }

Object { move: (), playerID: 0, data: Uint8Array(1), signature: {}, stateHash: Uint8Array(32) }

Object { arcadeumContract: {}, gameContract: {}, tag: 1, data: Uint8Array(9), meta: {} }

Object { move: (), playerID: 1, data: Uint8Array(1), signature: {} }

Object { arcadeumContract: {}, gameContract: {}, tag: 2, data: Uint8Array(9), meta: {} }

Object { move: (), playerID: 0, data: Uint8Array(1), signature: {}, stateHash: Uint8Array(32) }

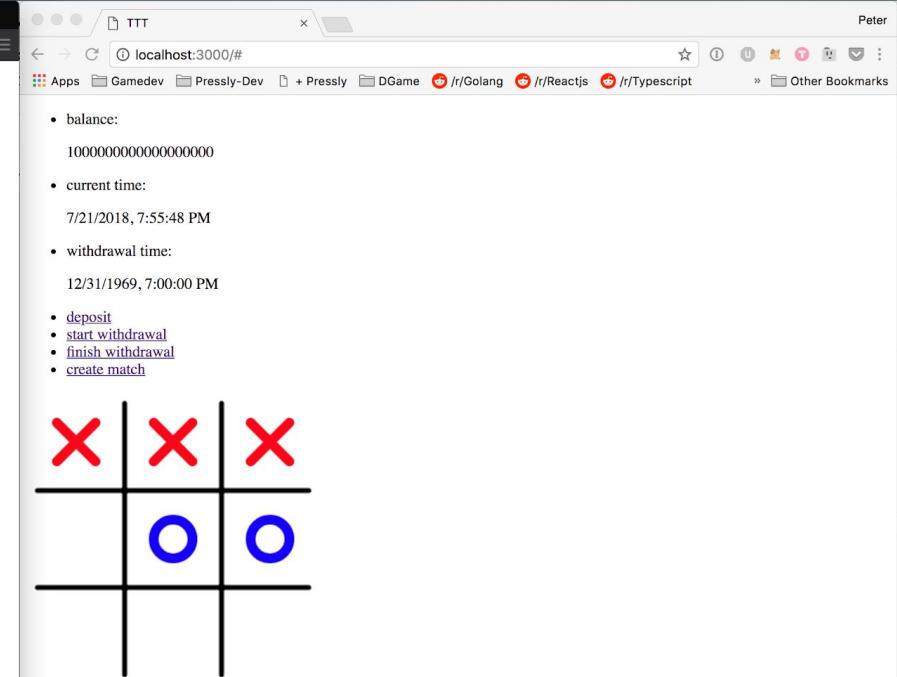
Object { arcadeumContract: {}, gameContract: {}, tag: 3, data: Uint8Array(9), meta: {} }

Object { move: (), playerID: 1, data: Uint8Array(1), signature: {} }

Object { arcadeumContract: {}, gameContract: {}, tag: 4, data: Uint8Array(9), meta: {} }

Object { move: (), playerID: 0, data: Uint8Array(1), signature: {}, stateHash: Uint8Array(32) }

Object { arcadeumContract: {}, gameContract: {}, tag: 5, data: Uint8Array(9), meta: {} }



BasicMatch {secretSeed: Uint8Array(), arcadeumContract: Contract, gameContract: Contract, serverAddress: "ws://localhost:8000/", signer: JsonRpcSigner, ...}

undefined

BasicState {arcadeumContract: Contract, gameContract: Contract, tag: 0, data: Uint8Array(9), meta: {}}

BasicMove {move: (), playerID: 0, data: Uint8Array(1), signature: Signature}

BasicState {arcadeumContract: Contract, gameContract: Contract, tag: 1, data: Uint8Array(9), meta: {}}

BasicMove {move: (), playerID: 1, data: Uint8Array(1), signature: Signature, stateHash: Uint8Array(32)}

BasicState {arcadeumContract: Contract, gameContract: Contract, tag: 2, data: Uint8Array(9), meta: {}}

BasicMove {move: (), playerID: 0, data: Uint8Array(1), signature: Signature}

BasicState {arcadeumContract: Contract, gameContract: Contract, tag: 3, data: Uint8Array(9), meta: {}}

BasicMove {move: (), playerID: 1, data: Uint8Array(1), signature: Signature, stateHash: Uint8Array(32)}

BasicState {arcadeumContract: Contract, gameContract: Contract, tag: 4, data: Uint8Array(9), meta: {}}

BasicMove {move: (), playerID: 0, data: Uint8Array(1), signature: Signature}

BasicState {arcadeumContract: Contract, gameContract: Contract, tag: 5, data: Uint8Array(9), meta: {}}

# State Channel Games — what else..

- Hub state availability
- Hub match persistence
- Hub optimized proofs
- Reward faucet
- Gas abstraction
- Plasma & side chains

Thank you!

<https://HorizonGames.net> / <https://SkyWeaver.net> / <https://arcadeum.net>



HONOR



WISDOM



STRENGTH



PURPOSE



COURAGE