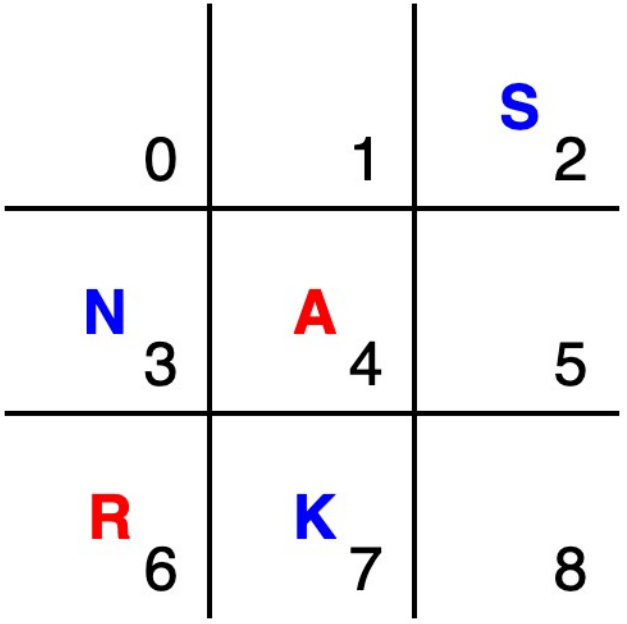
# Who?

Andrey Sobol
Mykhailo Tiutin
Alexander Kurbatov

# What?




# Tic-tac-toe using ZK SNARK

# Why?


I've made a robot that screams!
AAAAAAAAAA
AAAAAAAAAA
WHY?
AAAA AAA
AAA AAAAA

# Why?

1. Privacy: user can hide game strategy

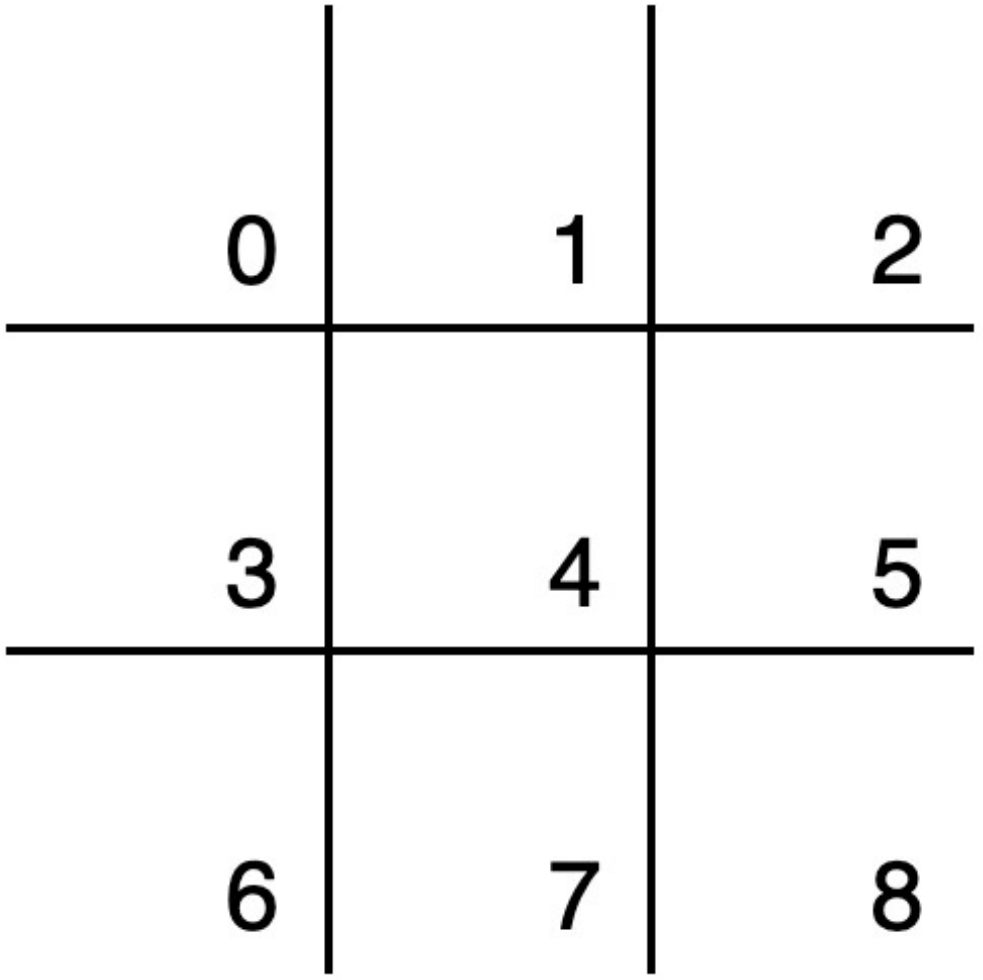
2. Scaling: we can publish onchain only final result with fixed size proof

# How?

1. ZoKrates
   (libsnark frontend)
   (zk lang .code)

2. ETH

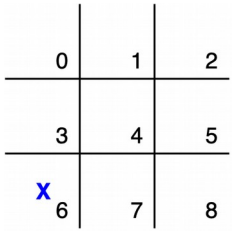
# Protocol




9 = Ø

Alice

Bob



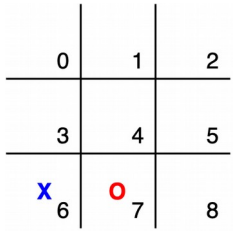

A=[6,9,9,9] A -> B

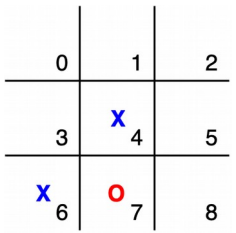
B=[9,9,9,9]

A <- B

A=[6,9,9,9]

B=[7,9,9,9]



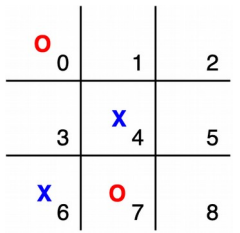

A=[6,4,9,9] A -> B

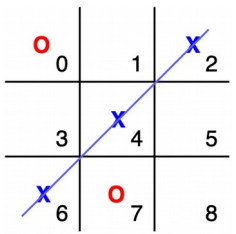
B=[7,9,9,9]

A <- B

A=[6,4,9,9]

B=[7,0,9,9]




pw/A/=[6,4,9,9]

pl/B/=[7,0,9,9]

c=2

A-> Zk Proof -> Smart contract

pw/A/=[6,4,9,9]

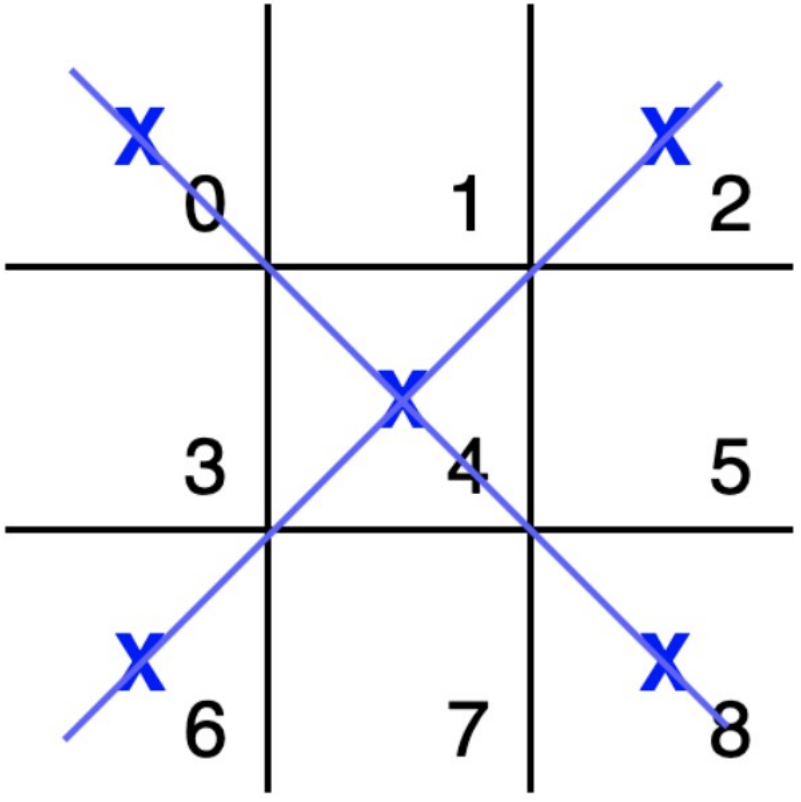
pl/B/=[7,0,9,9]

c=2

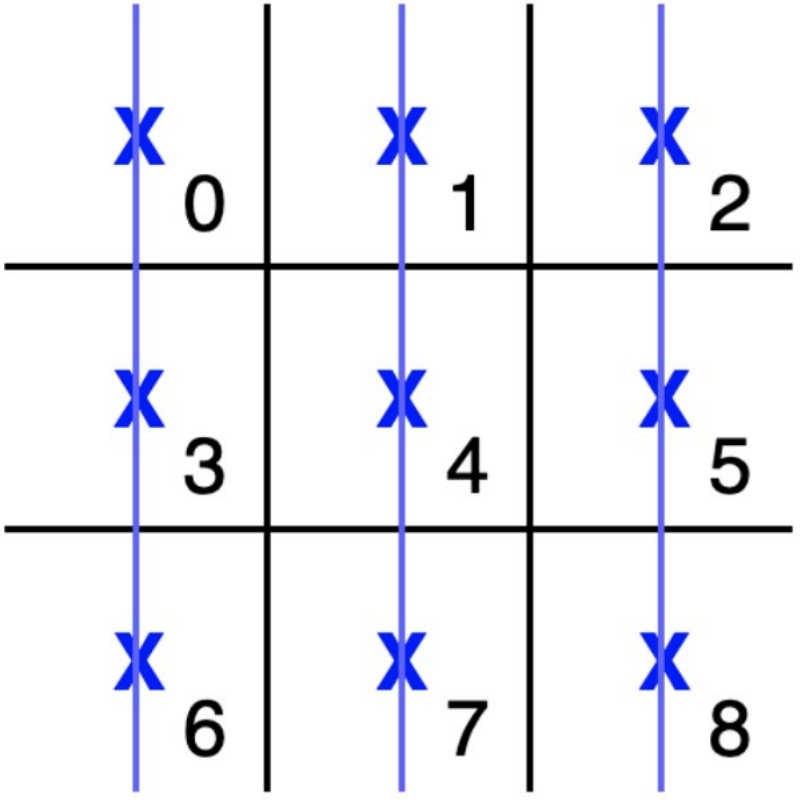
```
sigB(pw/A/=[6,4,9,9]
     pl/B/=[7,0,9,9])
c=2
```

$$\mathtt{hash}\left(\begin{matrix}\mathtt{pw/A/=[6,4,9,9]}\\ \mathtt{p1/B/=[7,0,9,9]}\end{matrix}\right)$$
$$\mathtt{c=2}$$

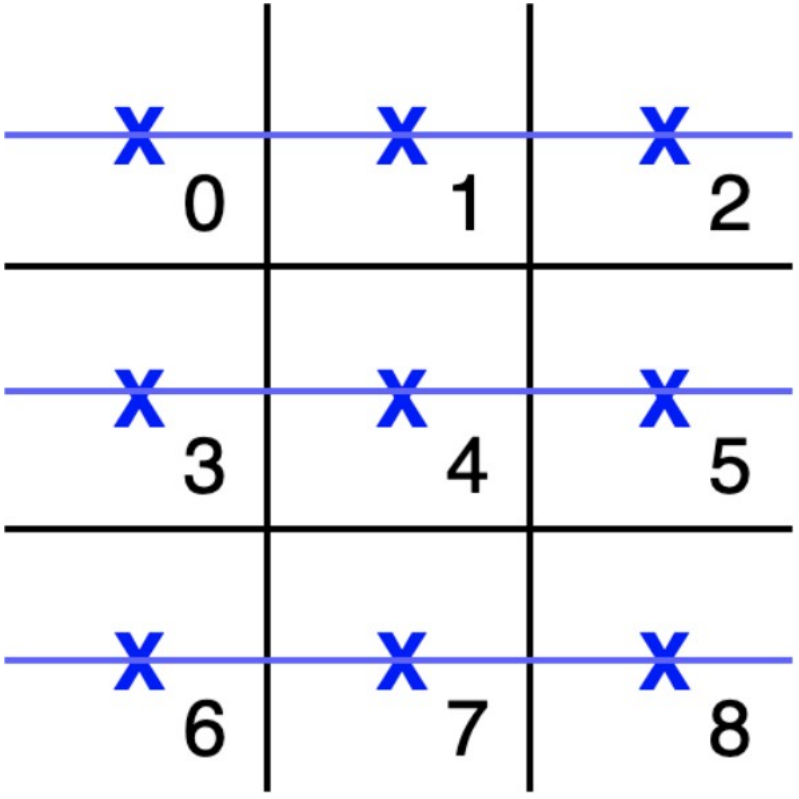
# Validation



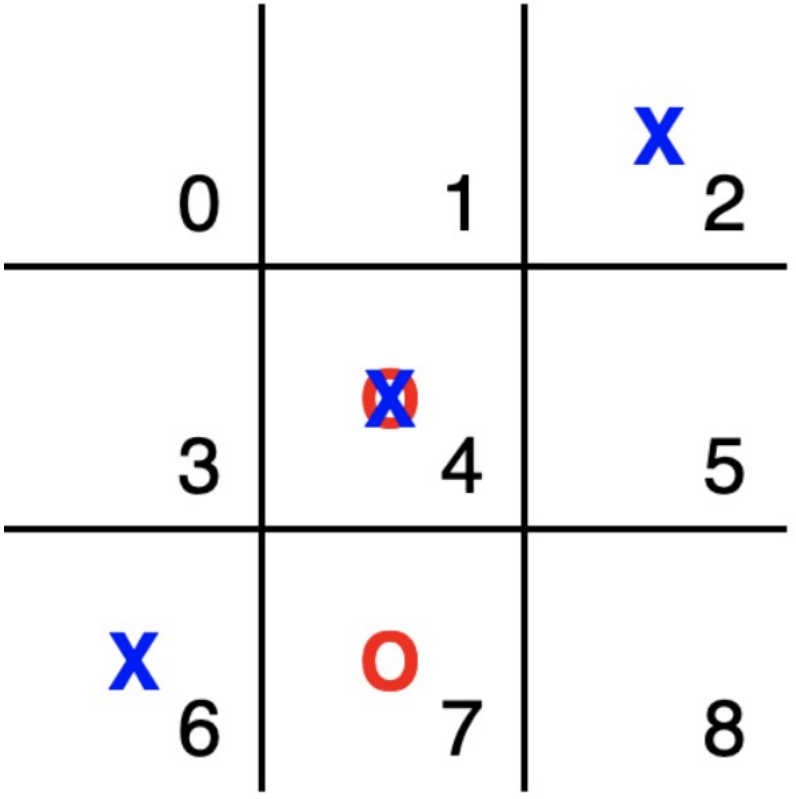

```
(0, 4, 8)
(2, 4, 6)
```




```
(0, 3, 6)
(1, 4, 7)
(2, 5, 8)
```




```
(0, 1, 2)
(3, 4, 5)
(6, 7, 8)
```




```
Move1 != Move2 or ((Move1==Ø) and (Move2==Ø))
```

## Main contition

```
pw + c ∈ (0, 1, 2) or
pw + c ∈ (3, 4, 5) or
...
pw + c ∈ (2, 4, 6)
```

# Thanks

https://github.com/andreysobol/tic-tac-toe-snark