EVALUATION OF ETHEREUM BLOCKCHAIN

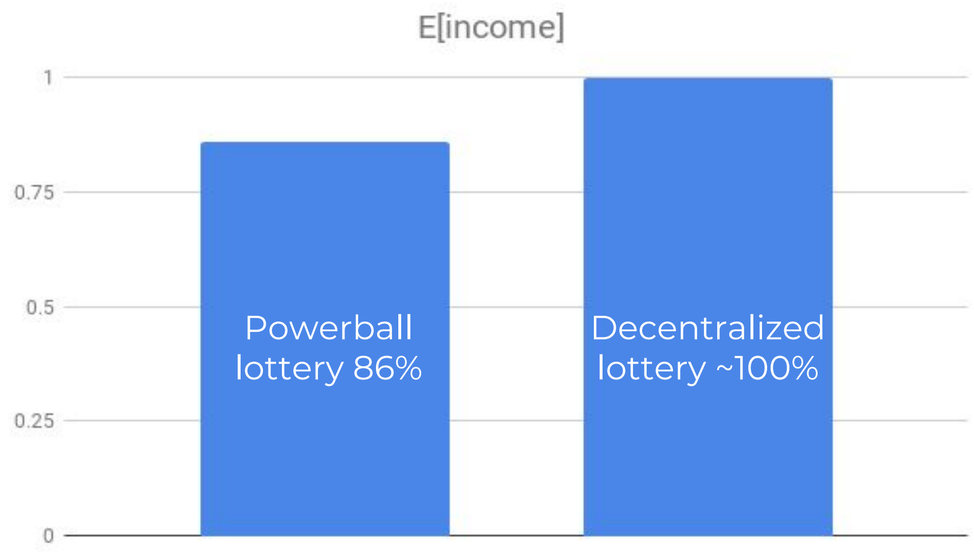
SMART CONTRACT LOTTERY APPLICATION

Lottery as a dApp

What is the problem we are trying to solve?

- Maximize income

E[income] = stake



- 100% not possible (gas cost)

Random Number Generation

Using random numbers in smart contracts is difficult if you don't want miners to be able to cheat.

Different solutions include:

- Using the blockhash
- Trusted third parties (Oraclize)
- Commitment scheme (commit, reveal, result)

There are limitations and tradeoffs in each of the different solutions!

Gas Cost

- Every operation costs gas
- Storing values more costly than doing operations
- Need to consider this when implementing

```javascript
var array = [];

function insert(value) {
  array.push(value);
}

function clear() {
  array = [];
}
```

Javascript

```
uint numElements = 0;
uint[] array;

function insert(uint value) {
    if(numElements == array.length) {
        array.length += 1;
    }
    array[numElements++] = value;
}

function clear() {
    numElements = 0;
}
```

Solidity

Blockchain Application: From Idea to Realization