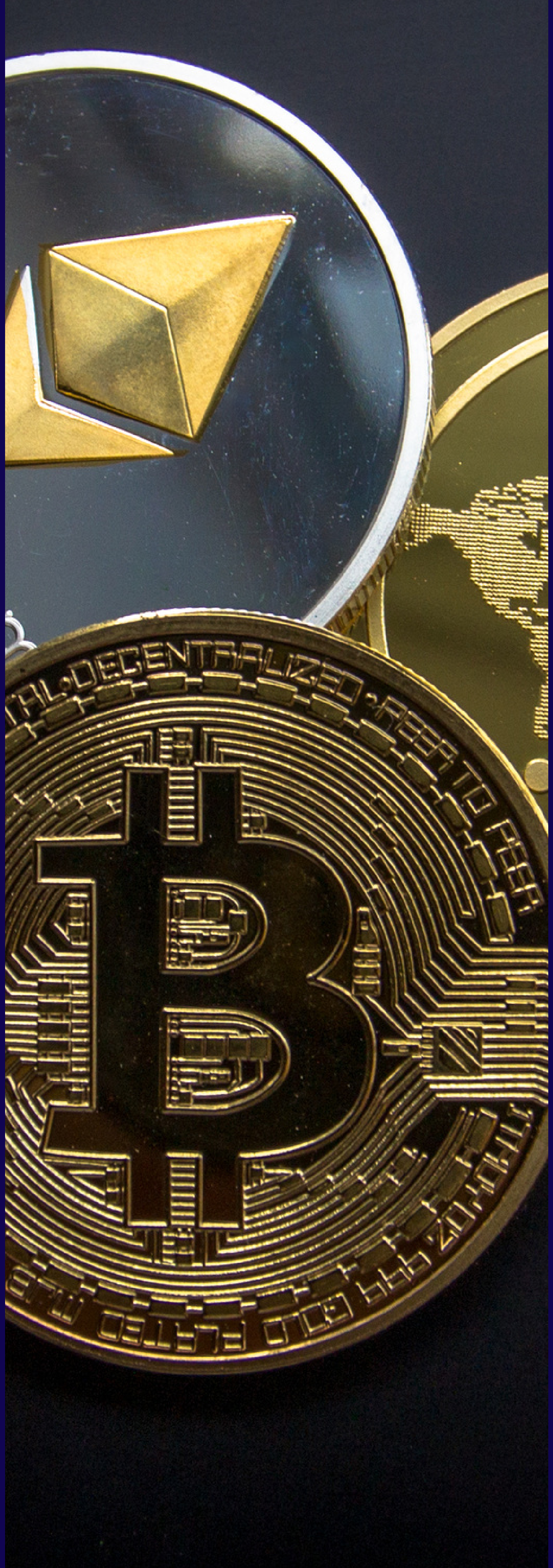


EXPLORING SECURITY & GAS USAGE OF SMART CONTRACTS THROUGH P2ES

PROBLEM

Security

- Vulnerabilities in smart contracts
- Stolen funds cannot be recovered

Gas Usage

- Inefficient code
- Transaction fees exceed value of transaction

CONTRIBUTIONS

1

Custom Security Scripts

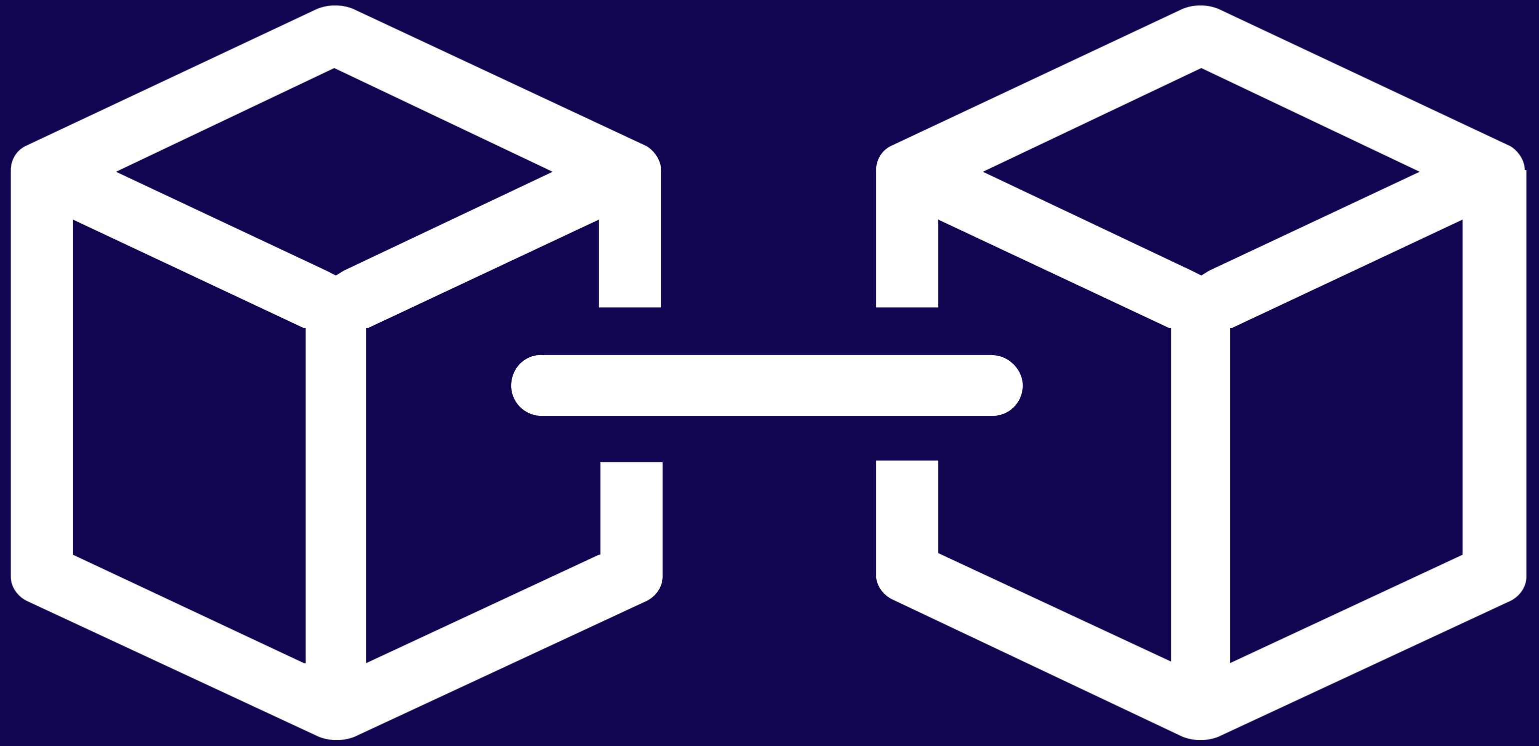
2

EVM Optimisations

3

NFT Price Prediction Model

BLOCKCHAIN



Axie Infinity

- Axie Infinity [1] is a virtual world of pets called Axies.
- Axies [1] can be collected and used to earn cryptocurrencies with real value.

Axie Infinity [2]

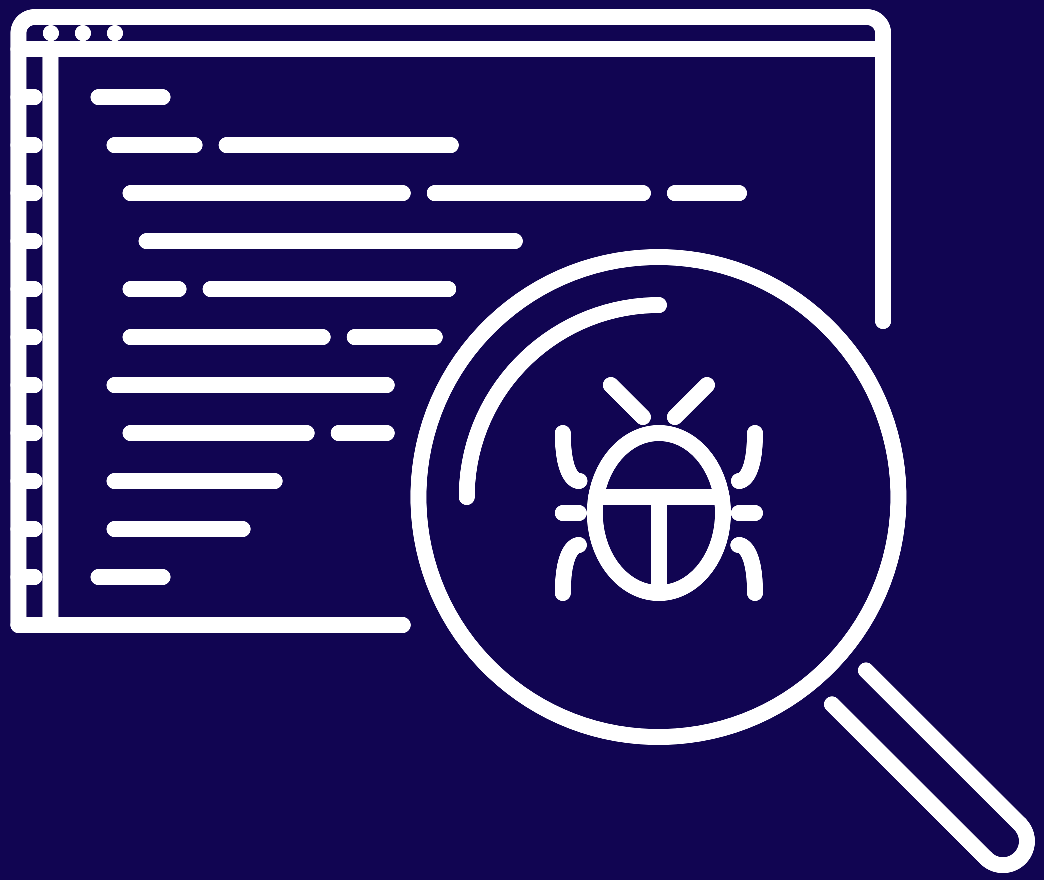
1. Sky Mavis. Welcome to Axie Infinity. https://welcome.axieinfinity.com [Accessed 20th June 2022].
2. Sky Mavis. Axie infinity. Axie Infinity. https://axieinfinity.com/ [Accessed 20th June 2022].

DEMONSTRATION

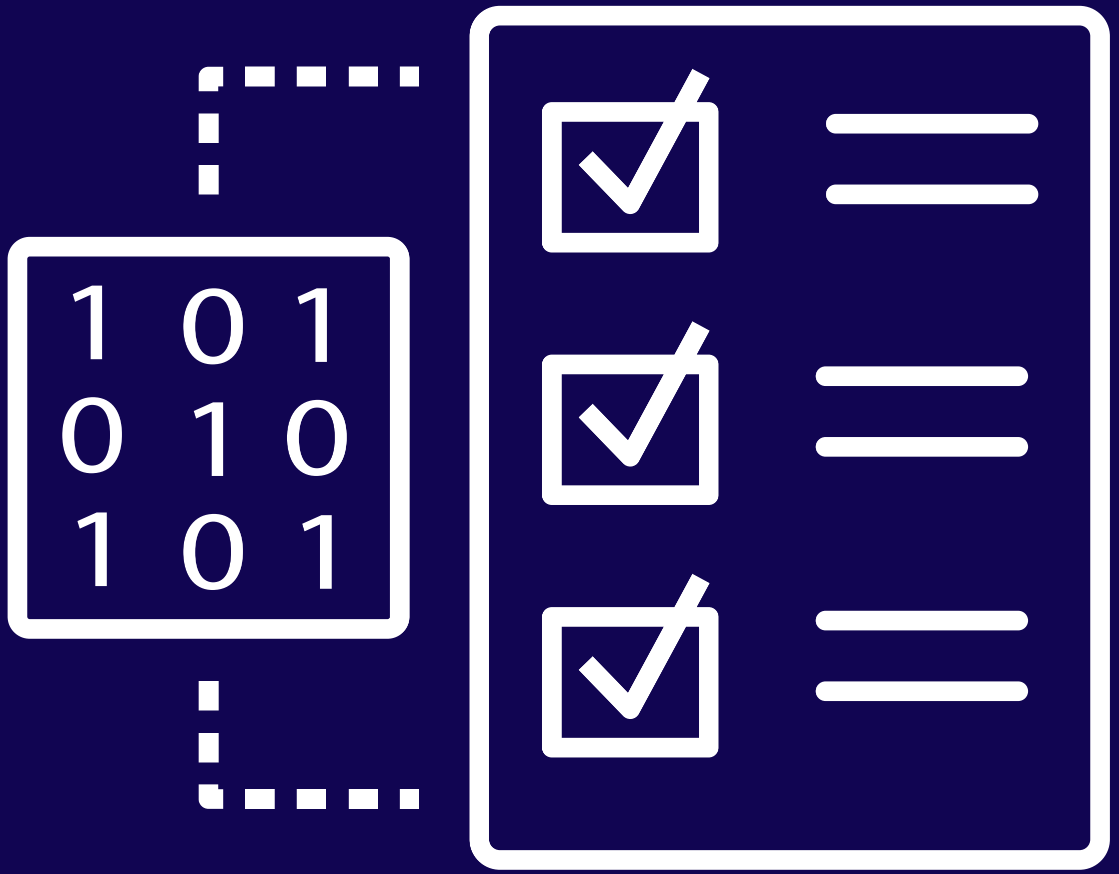
SECURITY

STATIC ANALYSIS

SLITHER



FUZZING



“

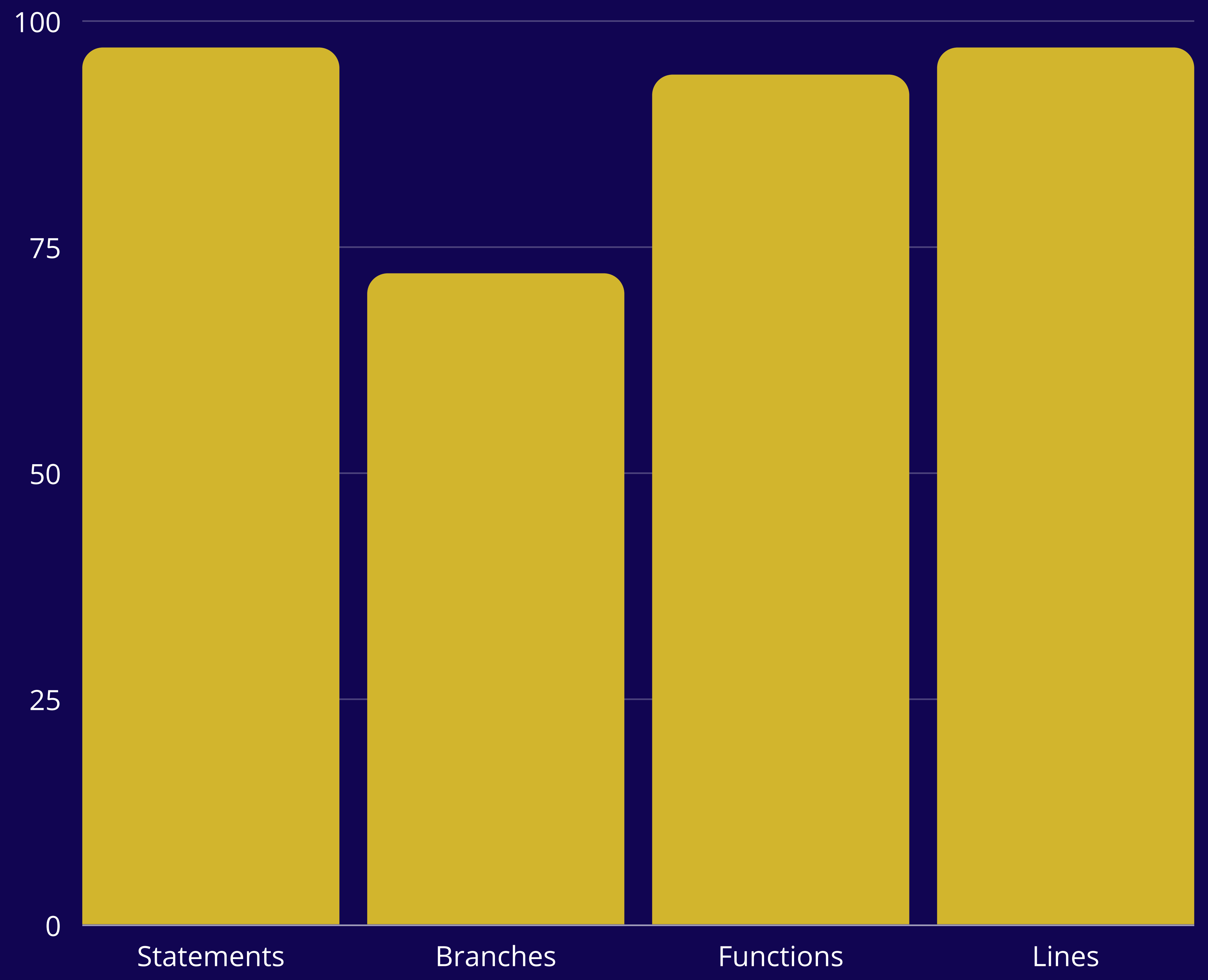
100% of invariants passing

”

TESTING

Hardhat

TEST COVERAGE



GAS OPTIMISATIONS

ASSEMBLY

OPCODE	GAS
ADD	3
MUL	5
SSTORE	> 2300

EVM Opcode Information [2]

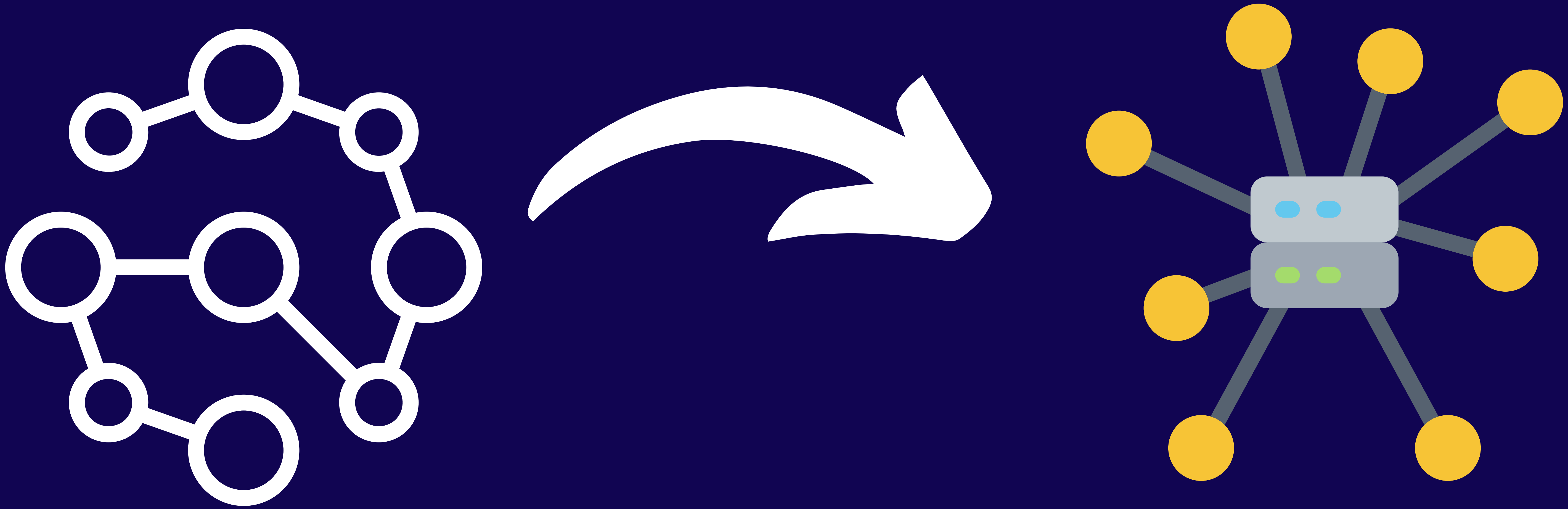
3. Wackerow P. Opcodes for the EVM. https://ethereum.org/en/developers/docs/evm/opcodes/ [Accessed 20th June 2022].

VARIABLE PACKING

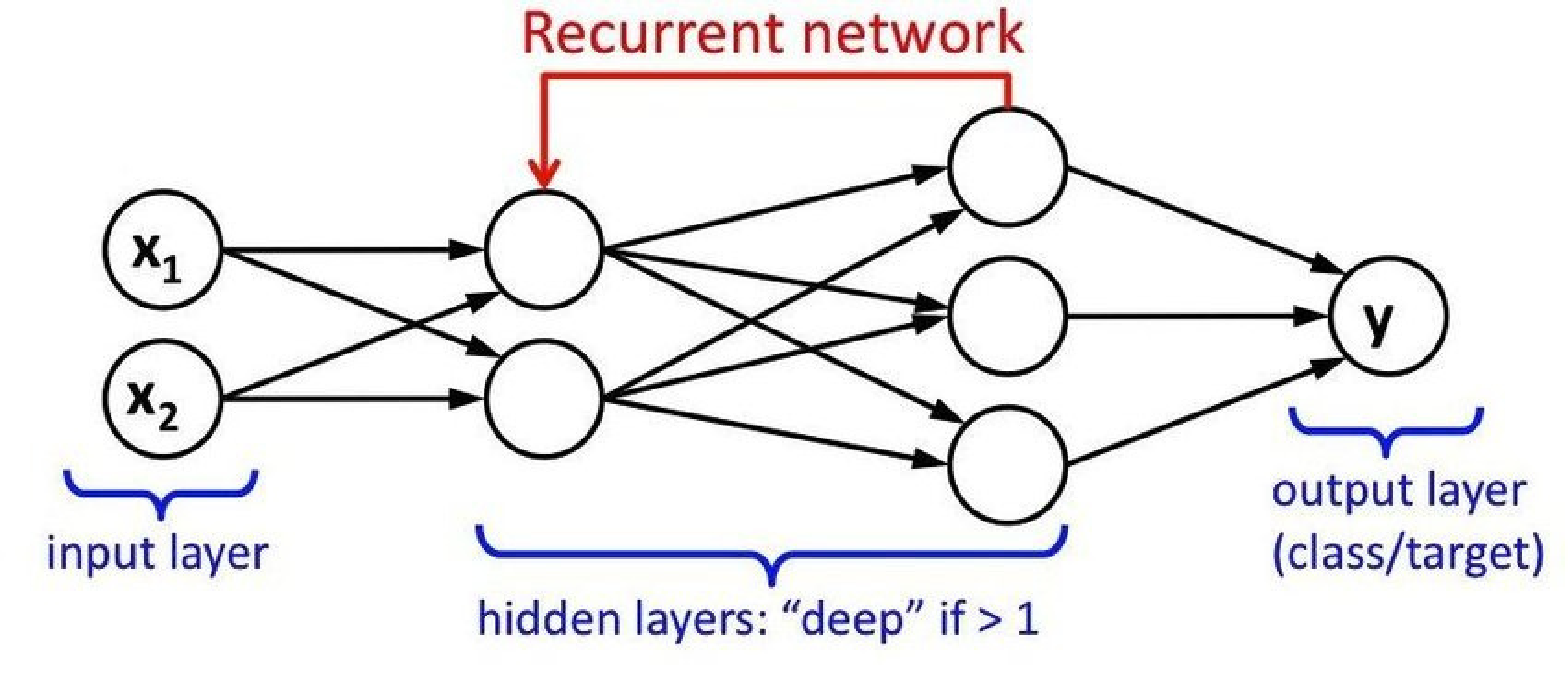
```
uint128 a1;
-----------------------------
uint256 b1;                // bad
-----------------------------
uint128 c1;


uint256 b2;
-----------------------------
uint128 a2;               // good
uint128 c2;
```

OFF-CHAIN



LSTM



Recurrent Neural Network [4]

4. Mishra V. Recurrent Network. ResearchGate. https://www.researchgate.net/figure/Recurrent-neural-networkRNN-or-Long-Short-Term-MemoryLSTM-5616_fig2_324883736 [Accessed 20th June 2022].

LSTM - RANDOM SEARCH

HYPERPARAMETER	RANGE	VALUE
# epochs	[32, 64, 256]	64
learning rate	$10^{-i}, \forall i \in [2,6)$	0.01
batch size	$2^{i}, \forall i \in [3,7)$	32
activation function	[tanh, sigmoid]	sigmoid
recurrent activation function	[tanh, sigmoid]	tanh

PRE PROCESS

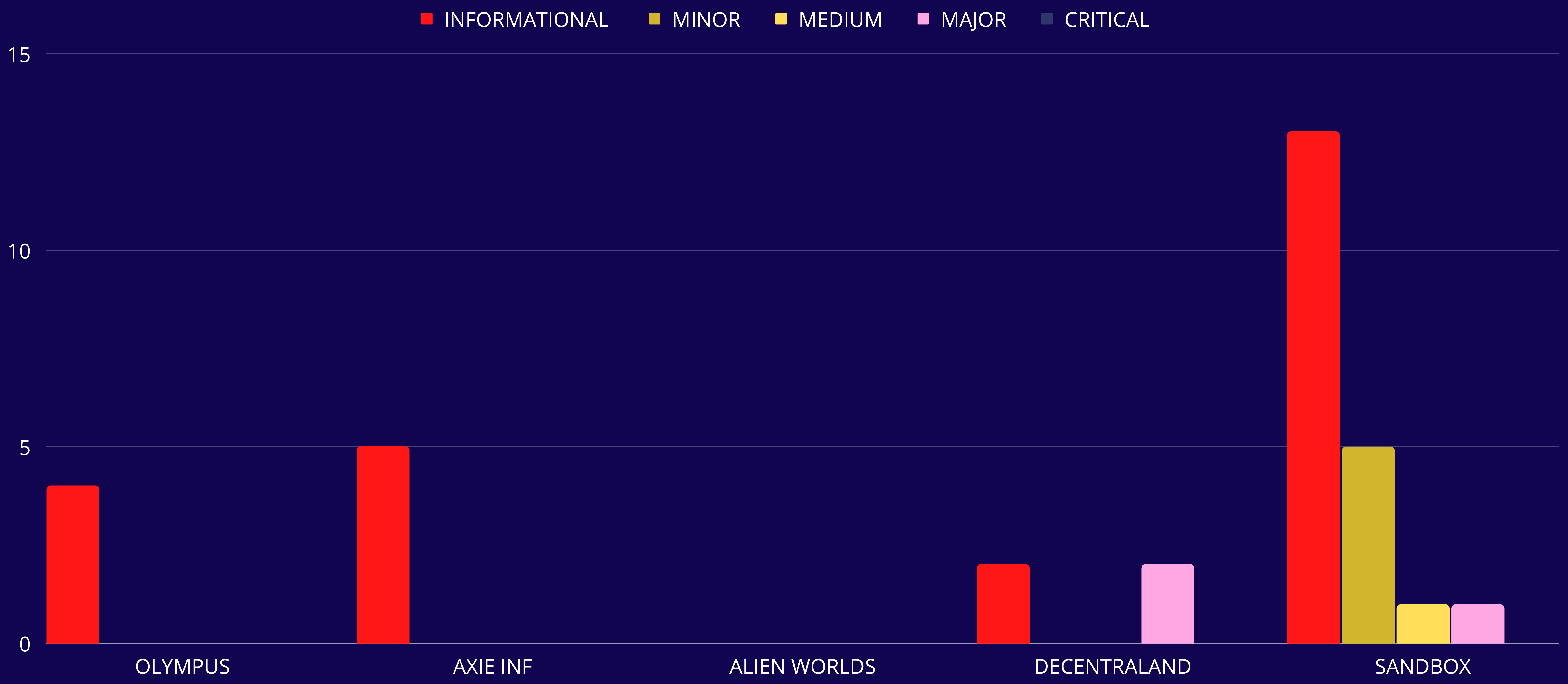
TRAIN MODEL

$f(x)$

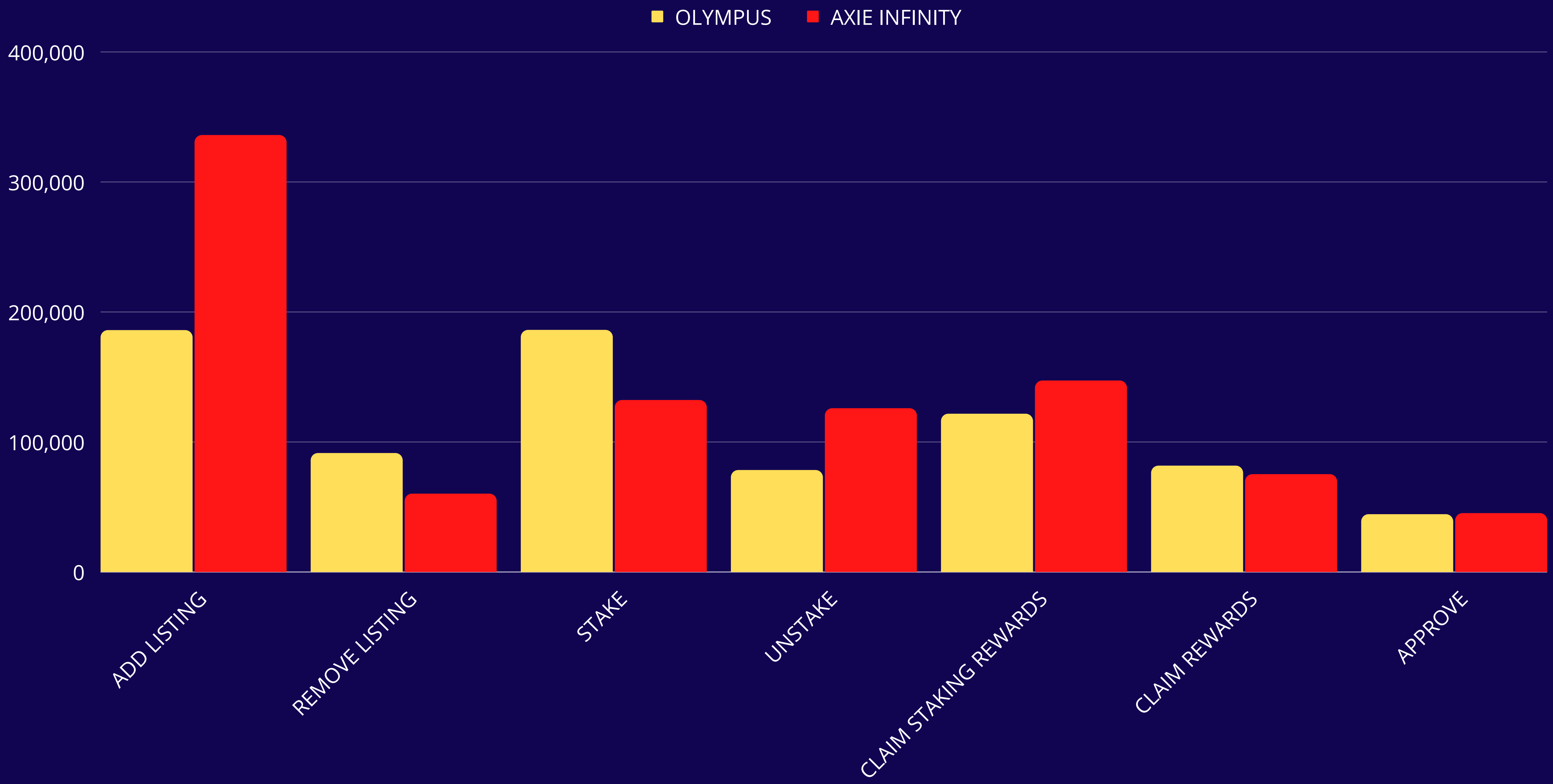
PREDICT

EVALUATION

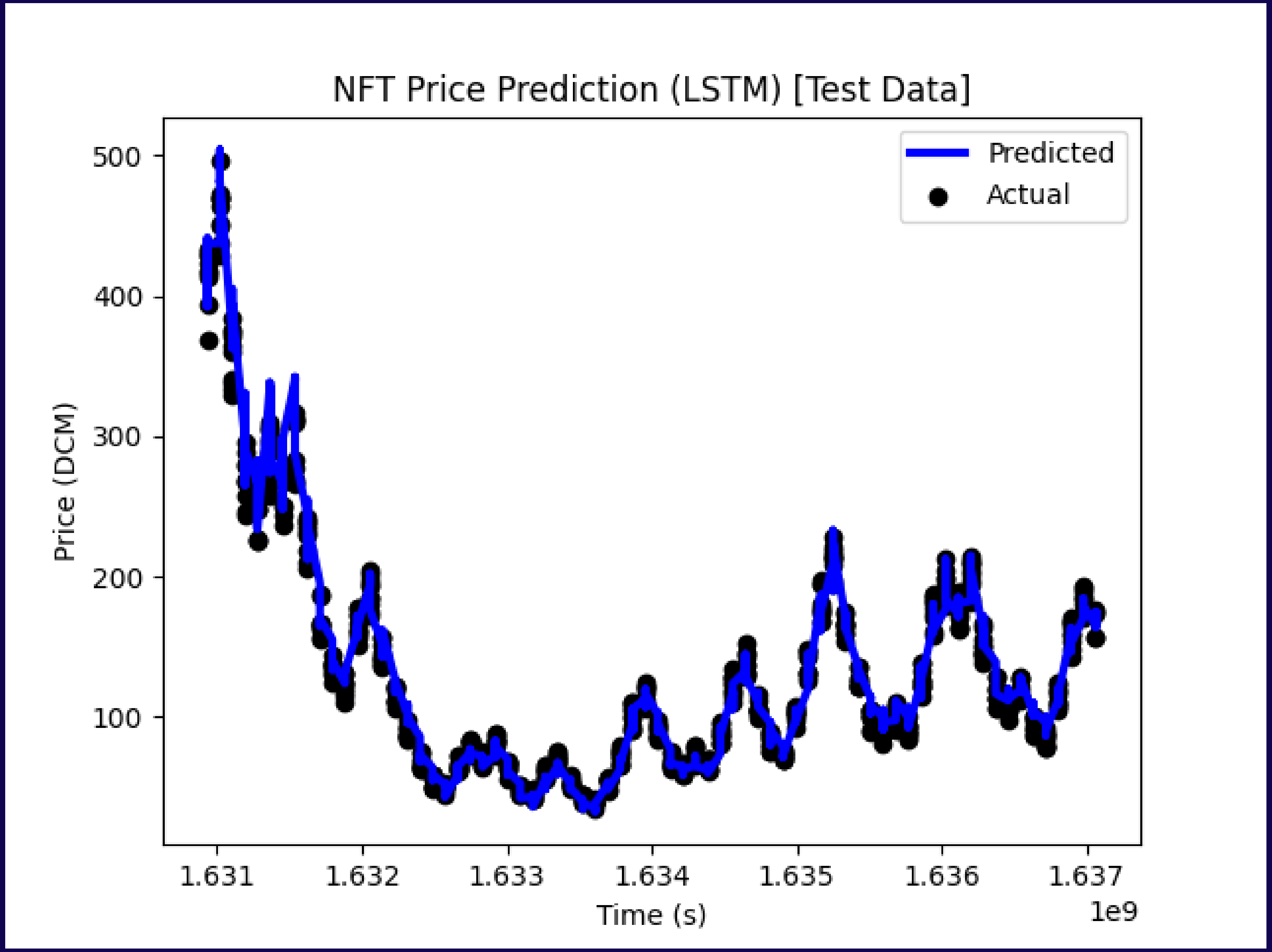
AUDIT REPORT



GAS COMPARISON



LSTM



MSE	R²
91.19	0.99

CONCLUSION

FUTURE WORK

QUESTIONS