RockEngine

PRIVACY VIRTUAL ENGINE

rockchain

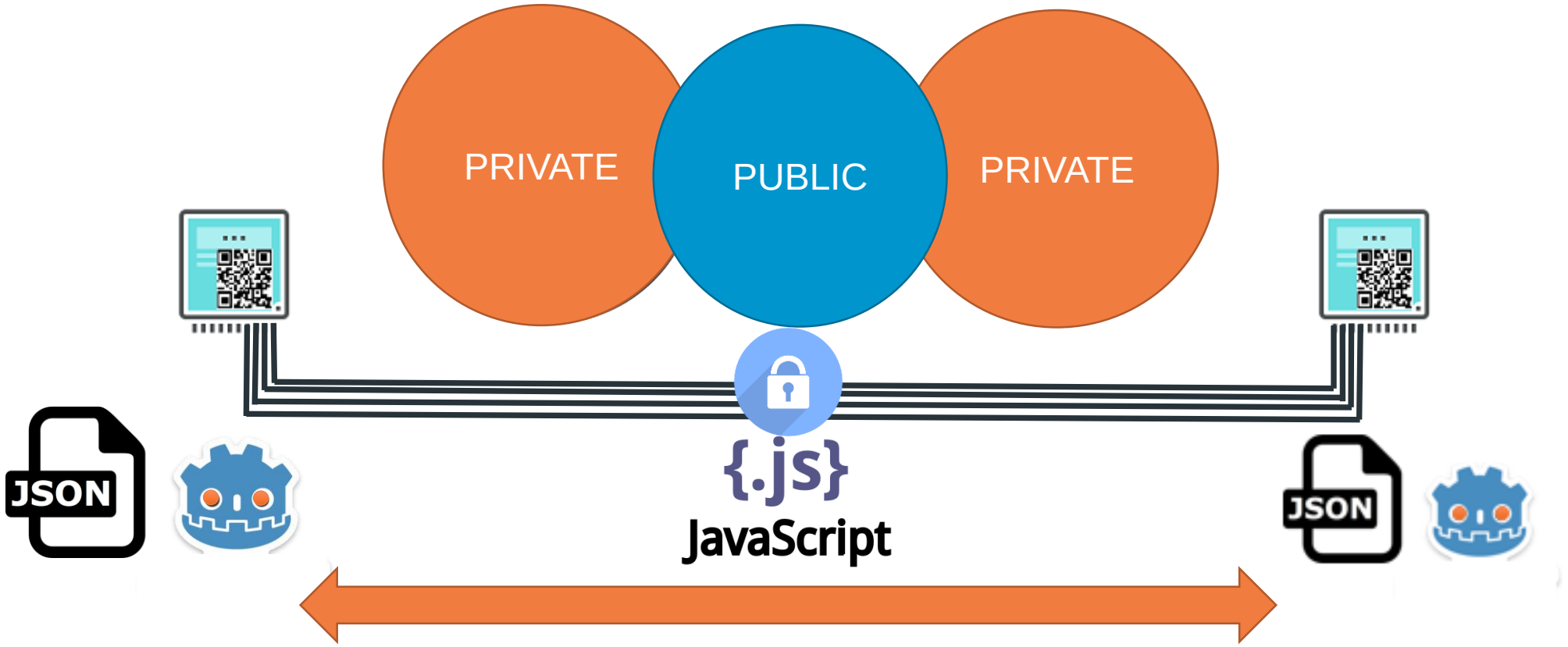
DISTRIBUTED DATA PRIVACY

RockEngine 2 PRIVATE NODES COMPUTATION

RockEngine is a distributed « virtual privacy engine » that can run scripts on 2 private nodes of a DappBox network to produce public data results.
The programing language is Javascript

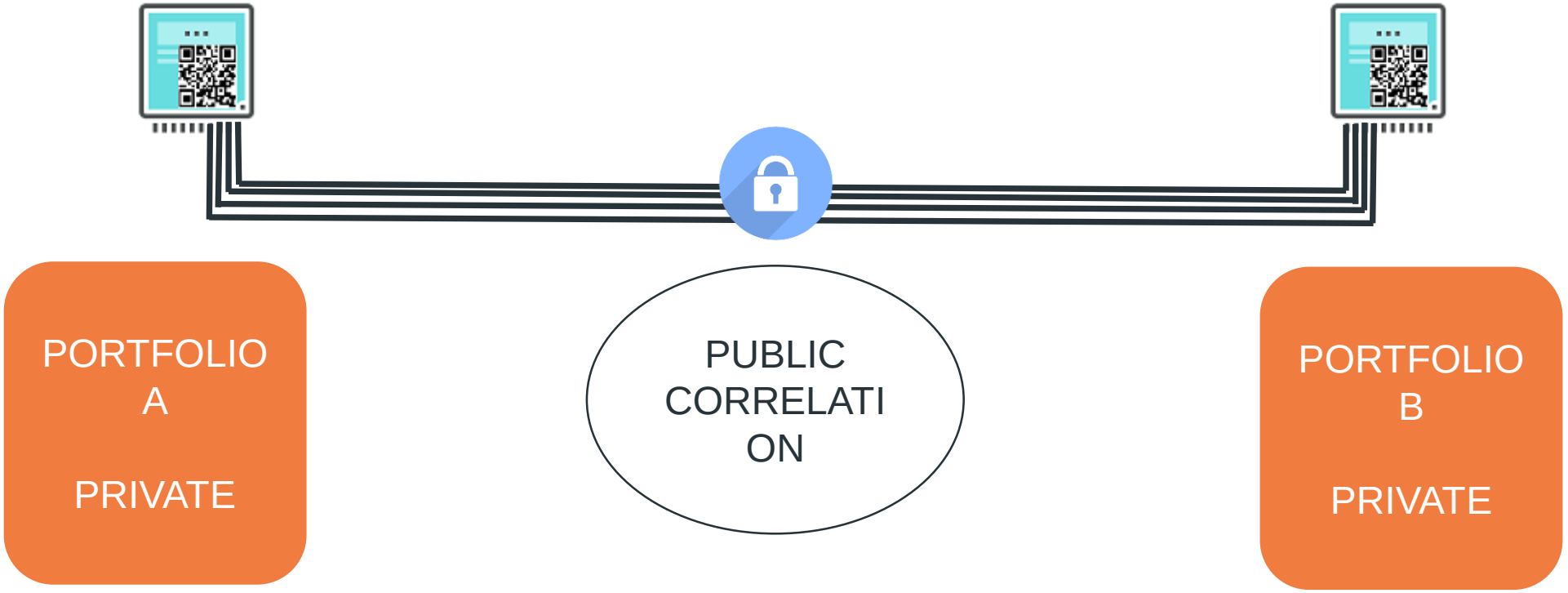
rockchain - **Distributed data privacy**

RockEngine Node 2 node computation



rockchain - Distributed data privacy

Use cases for finance: asset management



rockchain - **Distributed data privacy**

RockEngine Use cases for finance: Private equity

PRIVATE EQUITY INDUSTRY RATIOS ON PRIVATE DATABASE BY SECTORS

PUBLIC
PERCENTILES POSITION IN SECTOR PANEL
P/E (33%)
P/B (23%)
EV/SALES (25%)
EV/EBITDA (35%)
EV/EBIT (43%)

PRIVATE SOME ONLINE PROSPECT COMPANY ACCOUNTING RATIOS

rockchain - **Distributed data privacy**

RockEngine Use cases for authentication

Private bio-metrics based authentication systems (fingerprint, face and iris)

https://www.hindawi.com/journals/tswj/2014/525387/

RockEngine Use cases for dating

Privacy preserving dating site

https://courses.csail.mit.edu/6.857/2016/files/35.pdf/

The algorithmics

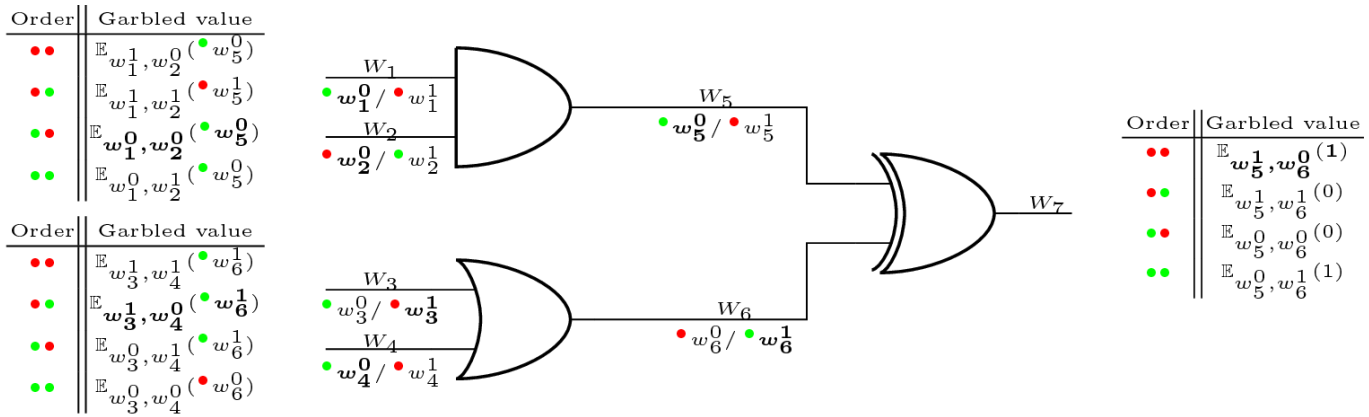


Figure 3: A circuit made of one AND gate and one OR gate and one XOR gate with their respective GTT and their labeled wires randomly colored. The bold values are the values used to compute the example below.

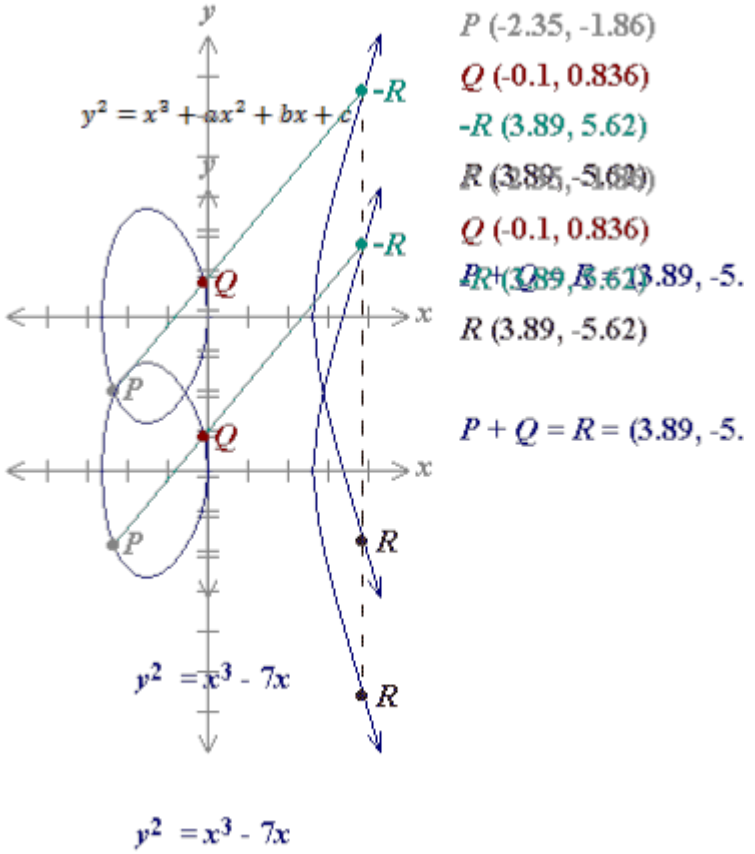
Background: Free-XOR

R

Global generator secret

$x^0 = A \qquad y^0 = B$

$x^1 = A \oplus R \qquad y^1 = B \oplus R$



Rockengine algorithm: security and performance

1. Benchmarked for memory usage performance http://rockchain.blog/benchmarking-computation-on-private-data-against-other-open-source-frameworks)

2. Verifiable computation: proof that the algorithm has not been modified on both sides

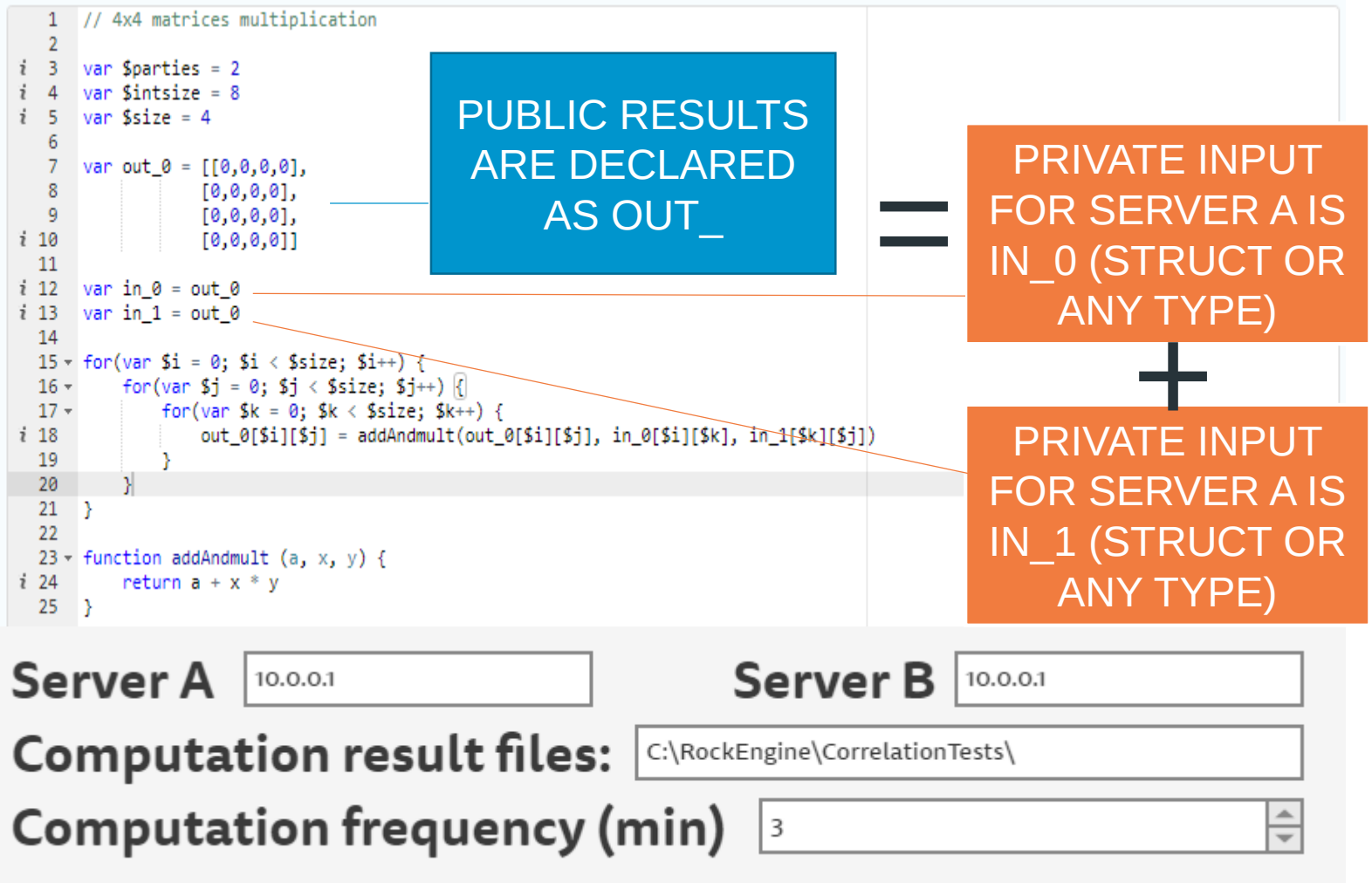
(https://eprint.iacr.org/2009/547.pdf)

3. Proof that the encrypted running algorithm is derived from a known source code.

3. Mathematically guarantee the privacy of computation inputs of both nodes

The tool in practice for developers

An online javascript editor to prepare batch actions on 2 remote servers



Rockengine compiler

TURING COMPLETE SCRIPTS

ANY ALGORITHM POSSIBLES (JAVASCRIPT)

BUT FINATE LOOPS, NO UNDETERMINATE STATE (SUCH AS IN ETHEREUM BLOCKCHAIN SOLIDITY)