

Rapport de projet de fin de module Sécurité et Technologies Blockchain

Ce projet consiste à développer une application décentralisée en utilisant Solidity pour la partie backend (smart contracts) et ReactJS pour l'interface utilisateur. Il s'inscrit dans le cadre d'un module portant sur les technologies blockchain et vise à mettre en pratique les notions de base de la programmation de contrats intelligents ainsi que leur interaction avec une interface web. Le projet repose sur l'environnement de développement Truffle, Ganache pour le réseau local Ethereum, et Web3.js pour la communication entre la blockchain et React.

L'application React que nous avons construite permet à l'utilisateur d'interagir avec différents contrats intelligents développés pour répondre à plusieurs exercices, chacun ciblant une notion spécifique de Solidity (les types de données, les fonctions, les chaînes de caractères, les structures de contrôle, les tableaux, les abstractions, etc.). L'utilisateur peut effectuer diverses opérations (par exemple : conversions, concaténations, vérifications, transferts) en appelant directement les fonctions des contrats via l'interface React.

Une partie complémentaire de l'application consiste à afficher des informations en temps réel sur l'état de la blockchain locale, telles que les détails du réseau, les transactions effectuées, les blocs minés, les adresses des comptes utilisés et les frais de gas. Cette section permet de mieux comprendre le fonctionnement interne d'une blockchain lors de l'exécution des contrats intelligents.

Pour illustrer ces différentes fonctionnalités, vous trouverez ci-dessous plusieurs captures d'écran de l'interface React développée, mettant en évidence l'interaction entre l'utilisateur, l'application web et la blockchain simulée.

Projet de Fin de Module

Développement d'une dApp pour le TP 3

Solidity, Truffle et ReactJS

- Exercice 1: Addition
- Exercice 2: Soustraction
- Exercice 3: Chaînes de caractères
- Exercice 4: Tableaux
- Exercice 5: Structures
- Exercice 6: Mappings
- Exercice 7: Enumérations
- Exercice 8: Les unités de temps, ether et gas

Ether	Convert Ether to Wei
Wei	Convert Wei to Ether

Accounts: 0xd01dbdc6Ada423af272f2877be7d6a91769db688, 0xe20128c58c47d4bc12d24f37e221e292190c9f5, 0x1214c4730eca60e687ba3b4044725f68571745, 0x1c8fefa2f060c19049420e15d61879f6a7da645, 0xd83a7a1ba54474789c854CaE575ef5C36938, 0xd232df2f605751914d545564a8695EeeA14a, 0xecf884B5313fA50DE13124f5F20Bd6d5ea9b908, 0x31C9e90D8425C59338CA4c290e440516664922E, 0x2bd017E0812c711223ACBD8D0c84a9aa189f7, 0xd8b36A91fcd64e0426e49d888999043f155fE

Informations de la Blockchain

Blockchain

URL : http://127.0.0.1:7545

ID : 5777

Compte : 0xd01dbdc6Ada423af272f2877be7d6a91769db688

N° : 19

Hash : 0x53226146c18f0b8103ccadc11835f27b008f378f8444ebd186ded94b899edf

Timestamp : 5/15/2025, 1:18:38 PM

parentHash : 0xd0fb1dee45d4403d99f731c5a39dfcd9f1691b3e961fa53666dcf30f2afc17

Transactions : 1

Miner : 0x00

Gas Limit : 6721975

Gas Used : 6721975

Size : 1268

Transactions (1)

Expéditeur : 0xd1dbdc6ada423af272f2b77be7d6a91769db688

Destinataire :

Montant : 0 ETH

Gas : 6721975

Hash : 0xed0bf7a81f639b79f56d2209f3b61d7b100f28e0f170eae0603c549899c29619

Bloc : 19

Fonction appelée (input) :

```
0x608060405234801561000075f806d5b50335f806101000a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff1602179055506102398061000c5f939f7f6e08060405234801561000075f806d5b506004361061003f5793360e01c8063445d0ac146100435780638da5c5b14610061578063f8ac5781461007f57935806d5b1610046100965656b60405161005891906101395656b60405180910390f3b6100696100a15656b604051610076919061015656b60405180910390f3b6100996100480360381019061009491906101d85656b100c4565b005b60015481565b5f8054906101000a900473ffffffffffffffffffffffffffffffffffffffff1681565b5f8054906101000a900473ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff163373ffffffffffffffffffffffffffffffffffffffff160361011e57806001819055505b56565819050919050565610133816101215656b25250505656b5f80208201905061014c5f83018461012a5656b291505056565f73ffffffffffffffffffffffffffffffffffffffff16021690509190505656561017b8261015254580909190505656101b81610115656b25250505656b5f8020820190506101a45f8301846101825656b29150505656565f806d5b6101b7816101215656b1146101c1575f80f45b5056565f813590506101d2816101ae5656b29150505656565f8020820312156101ed576101ec6d101aa56565656101fa848285016101c456565610509291505056f6a26469706673582122011e3f472c1d7652b23241c48ad44fc7cc3a465417ab3d64f14ce3cae28f91b64736f8c3430008150033
```

Projet de Fin de Module

Développement d'une dApp pour le TP 3

Solidity, Truffle et ReactJS

- Exercice 1: Addition
- Exercice 2: Soustraction
- Exercice 3: Chaînes de caractères
- Exercice 4: Tableaux
- Exercice 5: Structures
- Exercice 6: Mappings
- Exercice 7: Enumérations
- Exercice 8: Les unités de temps, ether et gas

Failed to connect to local blockchain

Informations de la Blockchain

Blockchain

URL : http://127.0.0.1:7545

ID : 5777

Compte : 0xd01dbdc6Ada423af272f2877be7d6a91769db688

N° : 19

Hash : 0x53226146c18f0b8103ccadc11835f27b008f378f8444ebd186ded94b899edf

Timestamp : 5/15/2025, 1:18:38 PM

parentHash : 0xd0fb1dee45d4403d99f731c5a39dfcd9f1691b3e961fa53666dcf30f2afc17

Transactions : 1

Miner : 0x00

Gas Limit : 6721975

Gas Used : 6721975

Size : 1268

Transactions (1)

Expéditeur : 0xd1dbdc6ada423af272f2b77be7d6a91769db688

Destinataire :

Montant : 0 ETH

Gas : 6721975

Hash : 0xed0bf7a81f639b79f56d2209f3b61d7b100f28e0f170eae0603c549899c29619

Bloc : 19

Fonction appelée (input) :

```
0x608060405234801561000075f806d5b50335f806101000a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff1602179055506102398061000c5f939f7f6e08060405234801561000075f806d5b506004361061003f5793360e01c8063445d0ac146100435780638da5c5b14610061578063f8ac5781461007f57935806d5b1610046100965656b60405161005891906101395656b60405180910390f3b6100696100a15656b604051610076919061015656b60405180910390f3b6100996100480360381019061009491906101d85656b100c4565b005b60015481565b5f8054906101000a900473ffffffffffffffffffffffffffffffffffffffff1681565b5f8054906101000a900473ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff163373ffffffffffffffffffffffffffffffffffffffff160361011e57806001819055505b56565819050919050565610133816101215656b25250505656b5f80208201905061014c5f83018461012a5656b291505056565f73ffffffffffffffffffffffffffffffffffffffff16021690509190505656561017b826101525656b90509190505656101b81610115656b25250505656b5f8020820190506101a45f8301846101825656b29150505656565f806d5b6101b7816101215656b1146101c1575f80f45b5056565f813590506101d2816101ae5656b29150505656565f8020820312156101ed576101ec6d101aa56565656101fa848285016101c456565610509291505056f6a26469706673582122011e3f472c1d7652b23241c48ad44fc7cc3a465417ab3d64f14ce3cae28f91b64736f8c3430008150033
```

Projet de Fin de Module

Développement d'une dApp pour le TP 3

Solidity, Truffle et ReactJS

- Exercice 1: Addition
- Exercice 2: Soustraction
- Exercice 3: Chaînes de caractères
- Exercice 4: Tableaux
- Exercice 5: Structures
- Exercice 6: Mappings
- Exercice 7: Enumérations
- Exercice 8: Les unités de temps, ether et gas

Exercice 4 - Check if Number is Positive

Informations de la Blockchain

Blockchain

URL : http://127.0.0.1:7545

ID : 5777

Compte : 0xD1dbdCb6AdA423aF272f2877Be7d6a91769dB688

N° : 19

Hash : 0x53226146c18f0b8103ccad11835f27b008f378f8f4d4ebd186ded94b899edf

Timestamp : 5/15/2025, 1:18:38 PM

parentHash : 0x0dfb1fdee45d4403d99f731c5a39dfcc9f1691b3e961fa53666dc30f2afc17

Transactions : 1

Miner : 0x00

Gas Limit : 6721975

Gas Used : 6721975

Size : 1268

Transactions (1)

Expéditeur : 0xd1dbdcb6ada423af272f2b77be7d6a91769db688

Destinataire :

Montant : 0 ETH

Gas : 6721975

Hash : 0xed0bf7a81f639b79f564d209f3b61d7b100f28e0f170eae603c549899c29619

Bloc : 19

Fonction appelée (input) :

```
0x608060405234801561000575f806d5b50335f806101000a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff1602179055506102398061005c3f95f9f6e608060405234801561000575f806d5b506004361061003f5793560e01c8063445f80ac146100435780638da5c5b146100615780638da5c5b1461007575b580634610046e10096e693b604051610025b9190610139563b6040518091039f0f3b6100696100a1565360405161007691950610191563b6040518091039f0f3b61009960480360381019061009491906101d8565b6100c4565b005b60015481565b5f8054906101000a900473ffffffffffffffffffffffffffffffffffffffff1681565b5f8054906101000a900473ffffffffff1673ffffffffffffffffffffffffffffffffffffffff16373ffffffffffffffffffffffffffffffffffffffff160361011e57806001819055505b50565b5819050919050565b61013381610121565b822505056b5960208201905061014c5f803018461012a565b92915050565b5f73ffffffffffffffffffffffffffffffffffffffff2169050919050565b581017b2610152565b9050919050565b61018b81610171565b822505056b5b5f8020820190506101a45f8030184610182565b92915050565b5f806f5b6101b781610121565b81146101c1575f806f5b50565b5813590506101d2816101ae565b92915050565b5f802082840312156101ed576101ec6101aa565b5b5f6101fa848285016101c4565b9150509291505056fea264697066735822122011e3472c1d7652b23241c48ad444cb7cc3a465417ab3d64f14ce3cae28fb91b64736f6cd3430008150033
```

Projet de Fin de Module

Développement d'une dApp pour le TP 3

Solidity, Truffle et ReactJS

- Exercice 1: Addition
- Exercice 2: Soustraction
- Exercice 3: Chaînes de caractères
- Exercice 4: Tableaux
- Exercice 5: Structures
- Exercice 6: Mappings
- Exercice 7: Enumérations
- Exercice 8: Les unités de temps, ether et gas

Exercice 5 - Check if Number is Even

Informations de la Blockchain

Blockchain

URL : http://127.0.0.1:7545

ID : 5777

Compte : 0xD1dbdCb6AdA423aF272f2877Be7d6a91769dB688

N° : 19

Hash : 0x53226146c18f0b8103ccad11835f27b008f378f8f4d4ebd186ded94b899edf

Timestamp : 5/15/2025, 1:18:38 PM

parentHash : 0x0dfb1fdee45d4403d99f731c5a39dfcc9f1691b3e961fa53666dc30f2afc17

Transactions : 1

Miner : 0x00

Gas Limit : 6721975

Gas Used : 6721975

Size : 1268

Transactions (1)

Expéditeur : 0xd1dbdcb6ada423af272f2b77be7d6a91769db688

Destinataire :

Montant : 0 ETH

Gas : 6721975

Hash : 0xed0bf7a81f639b79f564d209f3b61d7b100f28e0f170eae603c549899c29619

Bloc : 19

Fonction appelée (input) :

```
0x608060405234801561000575f806d5b50335f806101000a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff1602179055506102398061005c3f95f9f6e608060405234801561000575f806d5b506004361061003f5793560e01c8063445f80ac146100435780638da5c5b146100615780638da5c5b1461007575b580634610046e10096e693b604051610025b9190610139563b6040518091039f0f3b6100696100a1565360405161007691950610191563b6040518091039f0f3b61009960480360381019061009491906101d8565b6100c4565b005b60015481565b5f8054906101000a900473ffffffffffffffffffffffffffffffffffffffff1681565b5f8054906101000a900473ffffffffff1673ffffffffffffffffffffffffffffffffffffffff16373ffffffffffffffffffffffffffffffffffffffff160361011e57806001819055505b50565b5819050919050565b61013381610121565b822505056b5960208201905061014c5f803018461012a565b92915050565b5f73ffffffffffffffffffffffffffffffffffffffff2169050919050565b581017b2610152565b9050919050565b61018b81610171565b822505056b5b5f8020820190506101a45f8030184610182565b92915050565b5f806f5b6101b781610121565b81146101c1575f806f5b50565b5813590506101d2816101ae565b92915050565b5f802082840312156101ed576101ec6101aa565b5b5f6101fa848285016101c4565b9150509291505056fea264697066735822122011e3472c1d7652b23241c48ad444cb7cc3a465417ab3d64f14ce3cae28fb91b64736f6cd3430008150033
```

- Exercice 1: Addition
- Exercice 2: Soustraction
- Exercice 3: Chaînes de caractères
- Exercice 4: Tableaux
- Exercice 5: Structures
- Exercice 6: Mappings
- Exercice 7: Enumérations
- Exercice 8: Les unités de temps, ether et gas

Exercice 6 - Array Management

Number to add Add Number

Array Elements:

Sum of Elements: Loading...

Index to get Get Element

Informations de la Blockchain

Blockchain

URL : <http://127.0.0.1:7545>

ID : 5777

Compte : 0xD1d8dCb6Ada423af272f28778e7d6a91769d8688

N° : 19

Hash : 0x53226146c18f0b8103ccadc11835f27b008f378f8f44ebd186ded94b899edf

Timestamp : 5/15/2025, 1:18:38 PM

parentHash : 0xd8b1fdee45d4403d99f731c5a39dfcd9f1691b3e961fa53666dc30f2afc17

Transactions : 1

Miner : 0x00

Gas Limit : 6721975

Gas Used : 6721975

Size : 1268

Transactions (1)

Expéditeur : 0xd1dbdc6b6ada423af272f28778e7d6a91769db688

Destinataire :

Montant : 0 ETH

Gas : 6721975

Hash : 0xed0bf7a81f639b79f56d2209f3b61d7b100f28e0f170eae0603c549899c29619

Bloc : 19

Fonction appelée (input) :

```
0x0806040522480156100095758f06f5b50335f806101000a81548173ffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffff160217905550610239806
1005c5f395f9f3e60806040523480156100095758f06f5b506004361061003357f3560e01c8063445d0ac146100435780638da5cb5b14610061578063f8dcd376146100757
5b58f0d5b61004b61009b5656b6040516100589190610139562b60405180910390f35b100696100a1565b6040516100769190610191565b60405180910390f35b100996
0048036038101906100949190610148565b6100c4565b605b60015481565b5f8054906101000a900473ffffffffffffffffffffffffffffffff1681565b5f8054906101000a900473f
ffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffff163373ffffffffffffffffffffffffffffffff160361011e57806001819055505b5f819050919050565b61013
381610121565b82525050565b5f60208201905061014c5f83018461012a565b62915050565b5f73ffffffffffffffffffffffffffffffff162169050919050565b5f61017b826101525
65b9050919050565b61018b81610171565b82525050565b5f6020820190506101a45f830184610182565b62915050565b5f806d5b6101b781610121565b81146101c1575f
806d5b50565b5f813590506101d2816101ae565b62915050565b5f602082040312156101e4576101ec6101aa565b5b5f6101fa48285016101c4565b9150509291505056f6
a26469706673582122011e3f472c1d7652b23241c48ba44f1cc3a465417ab3d64f14ce3cae28fb91b64736f6c63430008150033
```

Page n° 8

- Exercice 1: Addition
- Exercice 2: Soustraction
- Exercice 3: Chaînes de caractères
- Exercice 4: Tableaux
- Exercice 5: Structures
- Exercice 6: Mappings
- Exercice 7: Enumérations
- Exercice 8: Les unités de temps, ether et gas

Exercice 7 - Rectangle

Position: $x = 0$, $y = 0$

Length:

Width:

Info:

Surface:

dx dy Move Shape

Informations de la Blockchain

Blockchain

URL : <http://127.0.0.1:7545>

ID : 5777

Compte : 0xD1d8dCb6Ada423af272f28778e7d6a91769d8688

N° : 19

Hash : 0x53226146c18f0b8103ccadc11835f27b008f378f8f44ebd186ded94b899edf

Timestamp : 5/15/2025, 1:18:38 PM

parentHash : 0xd8b1fdee45d4403d99f731c5a39dfcd9f1691b3e961fa53666dc30f2afc17

Transactions : 1

Miner : 0x00

Gas Limit : 6721975

Gas Used : 6721975

Size : 1268

Transactions (1)

Expéditeur : 0xd1dbdc6b6ada423af272f28778e7d6a91769db688

Destinataire :

Montant : 0 ETH

Gas : 6721975

Hash : 0xed0bf7a81f639b79f56d2209f3b61d7b100f28e0f170eae0603c549899c29619

Bloc : 19

Fonction appelée (input) :

```
0x0806040522480156100095758f06f5b50335f806101000a81548173ffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffff160217905550610239806
1005c5f395f9f3e60806040523480156100095758f06f5b506004361061003357f3560e01c8063445d0ac146100435780638da5cb5b14610061578063f8dcd376146100757
5b58f0d5b61004b61009b5656b6040516100589190610139562b60405180910390f35b100696100a1565b6040516100769190610191565b60405180910390f35b100996
0048036038101906100949190610148565b6100c4565b605b60015481565b5f8054906101000a900473ffffffffffffffffffffffffffffffff1681565b5f8054906101000a900473f
ffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffff163373ffffffffffffffffffffffffffffffff160361011e57806001819055505b5f819050919050565b61013
381610121565b82525050565b5f60208201905061014c5f83018461012a565b62915050565b5f73ffffffffffffffffffffffffffffffff162169050919050565b5f61017b826101525
65b9050919050565b61018b81610171565b82525050565b5f6020820190506101a45f830184610182565b62915050565b5f806d5b6101b781610121565b81146101c1575f
806d5b50565b5f813590506101d2816101ae565b62915050565b5f602082040312156101e4576101ec6101aa565b5b5f6101fa48285016101c4565b9150509291505056f6
a26469706673582122011e3f472c1d7652b23241c48ba44f1cc3a465417ab3d64f14ce3cae28fb91b64736f6c63430008150033
```

Page n° 9

- Exercice 1: Addition
Exercice 2: Soustraction
Exercice 3: Chaînes de caractères
Exercice 4: Tableaux
Exercice 5: Structures
Exercice 6: Mappings
Exercice 7: Enumérations
Exercice 8: Les unités de temps, ether et gas

Exercice 8 - Ether Wallet

Recipient:

Contract Balance: 0 ETH

 Amount in ETH

Your account: 0xD1dBdCb6Ada423af272f2877Be7d6a91769dB688

Informations de la Blockchain

Blockchain

URL : <http://127.0.0.1:7545>

ID : 5777

Compte : 0xD1dBdCb6Ada423af272f2877Be7d6a91769dB688

N° : 19

Hash : 0x53226146c18f0b8103ccade11835f27b008f378f8f4d4ebd186ded94b899edf

Timestamp : 5/15/2025, 1:18:38 PM

parentHash : 0xdfb1fdee45d4403d99731c5a39dfcd9f1691b3e961fa53666dcd30f2afc17

Transactions : 1

Miner : 0x00

Gas Limit : 6721975

Gas Used : 6721975

Size : 1268

Transactions (1)

Expéditeur : 0xd1dbdcb6ada423af272f2b77be7d6a91769db688

Destinataire :

Montant : 0 ETH

Gas : 6721975

Hash : 0xed0bf7a81f639b79f56d2209f3b61d7b100f28e0f170eae0603c549899c29619

Bloc : 19

Fonction appelée (input) :

```
0x608060405234801561000f57580fd5b50335806101000a81548173ffffffffffffffffffffffffffffffffffffffff02191690b3373ffffffffffffffffffffffffffffffffffffffff160217905550610239061005c5f395f3fe608060405234801561000f57580fd5b506004361061003575f3560e01d063445df0ac146100435780638da5c5b14610061578063fda5c5b1461007575b5b80fd5b61004b61009b5656b6040516100589190610139562b60405180910390f35b6100696100a1565b6040516100769190610191565b60405180910390f35b61009960480360381019061009491906101d8565266100a4565605b60015481565258054906101000a900473ffffffffffffffffffffffffffffffffffffffff1681565258054906101000a900473ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff163373ffffffffffffffffffffffffffffffffffffffff160361011e57806001819055505b5f819050919050565b61013381610121565b6025205050565b5f60208201905061014c5f83018461012a565b62915050565b5f73ffffffffffffffffffffffffffffffffffffffff82169050919050565b5f61017b82610152565b9050919050565b61018b81610171565b82525050565b5f6020820190506101a45f830184610182565b62915050565b5f8045b6101b781610121565b81146101c1575f80fd5b50565b5f813390506101d281011e455f8a92915050565b5f602082040312156101e45781011e456101a56101b101a48205016101c4565091505092915050565ba264697066735822122011e3f472c1d7652b23241c48ad44fc7cc3a465417ab3d64f14ce3cae28f691b64736f6c63430008150033
```