

Concept demo (first draft)

https://legalsmartcontract.herokuapp.com

Situation : Alice want to sell Bob 20 bags of "Taro". She want to create a legal contract that require Bob's signature.

Before using this web application Alice and Bob have to generate a private/public keypair on Ethereum Blockchain in order to interact with the blockchain.

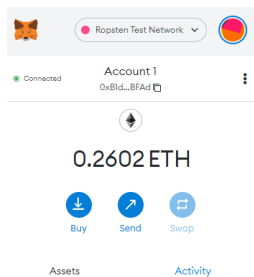
For this demo, these are their Ethereum address

Alice : 0xB1d1aE061e066AE70E2cC794938a619fE7FBFAAd

Bob : 0xFEfA7bea8457ed525F4120579f2dF852234274cC

Here is a short summary of how it work, Alice creates a contract on this web application, write Bob address as a recipient, sign and send it to the smart contract deployed on Ethereum test network. On Bob's side, the web application will search through all the contract inside this smart contract and return ALL contract that involve Bob. Bob selects the contract that is created by Alice, verify the hash of the contract detail, and then sign the contract (*smart contract code make sure that no one can sign this contract except Bob, and also make sure to Bob that Alice is the one who initiate this contract).

1. On first visit, Metamask will pop up asking Alice for permission to connect to this website (for this demo, use Ropsten test network)



2. Alice can edit the contract detail, then click "Generate new template" to generated the form automatically. (for this demo, any text wrapped by square bracket [...] will turn into a form)

[Home](#) | [view deployed contracts](#) |

ropsten test network : 0x8bd126632b72715929b1FE7DaF1Ea928D7D8d3B8

Editable Template	Form	Preview
<div>Generate new template</div> <p>**สัญญาซื้อขายขนม** [[ตัวเลือกขนม:Choice("หาโร","ซูทิส","จอลส์โคล่า")]] **[สัญญาซื้อขายขนม:ตัวเลือกขนม]**</p> <p>**ข้อ 1.** ผู้ขายตกลงขายและผู้ซื้อตกลงซื้อขนมของผู้ขาย จำนวน **[[จำนวนสินค้าที่สั่งซื้อ]]** ชิ้น รวมเป็นเงิน **[[จำนวนเงิน]]** บาท</p> <p>**ข้อ 2.** สำหรับราคาสินค้าส่วนนี้ผู้ซื้อตกลงชำระให้แก่ผู้ขายภายในวันที่ **[[กำหนดชำระเงิน:Date]]**</p> <p>**ข้อ 3.** หากผู้ขายได้รับเงินแล้ว จะต้องดำเนินการส่งสินค้าภายในเวลา **[[จัดส่งภายใน]]** วัน</p> <p>**ข้อ 4.** หากผู้สัญญาฝ่ายหนึ่งฝ่ายใดเกิดสัญญา ให้อีกฝ่ายหนึ่งมีสิทธิบอกเลิกสัญญาและมีสิทธิเรียกร้องค่าเสียหายจากฝ่ายที่ผิดสัญญาได้ตามความเป็นจริง</p> <p>ลงวันที่ **[[วันที่:Date]]**</p> <p>ลงชื่อ **[[ชื่อผู้ขาย]]** ผู้ขาย</p> <p>ลงชื่อ **[[ชื่อผู้ซื้อ]]** ผู้ซื้อ</p>	<div>สัญญาซื้อขายขนม</div> <div>— Please choose from the list —</div> <div>จำนวนสินค้าที่สั่งซื้อ</div> <div>จำนวนเงิน</div> <div>กำหนดชำระเงิน</div> <div>จัดส่งภายใน</div> <div>วันที่</div> <div>ชื่อผู้ขาย</div> <div>ชื่อผู้ซื้อ</div>	<div>Download PDF</div> <p>สัญญาซื้อขายขนม ____</p> <p>ข้อ 1. ผู้ขายตกลงขายและผู้ซื้อตกลงซื้อขนมของผู้ขาย จำนวน ____ ชิ้น รวมเป็นเงิน ____ บาท</p> <p>ข้อ 2. สำหรับราคาสินค้าส่วนนี้ผู้ซื้อตกลงชำระให้แก่ผู้ขายภายในวันที่ ____</p> <p>ข้อ 3. หากผู้ขายได้รับเงินแล้ว จะต้องดำเนินการส่งสินค้าภายในเวลา ____ วัน</p> <p>ข้อ 4. หากผู้สัญญาฝ่ายหนึ่งฝ่ายใดเกิดสัญญา ให้อีกฝ่ายหนึ่งมีสิทธิบอกเลิกสัญญาและมีสิทธิเรียกร้องค่าเสียหายจากฝ่ายที่ผิดสัญญาได้ตามความเป็นจริง</p> <p>ลงวันที่ ____</p> <p>ลงชื่อ ____ ผู้ขาย</p> <p>ลงชื่อ ____ ผู้ซื้อ</p> <div>SEND TO BLOCKCHAIN ></div>
<div>Generate new template</div> <p>**สัญญาซื้อขายขนม** [[ตัวเลือกขนม:Choice("หาโร","ซูทิส","จอลส์โคล่า")]] **[สัญญาซื้อขายขนม:ตัวเลือกขนม]**</p> <p>**ข้อ 1.** ผู้ขายตกลงขายและผู้ซื้อตกลงซื้อขนมของผู้ขาย จำนวน **[[จำนวนสินค้าที่สั่งซื้อ]]** ชิ้น รวมเป็นเงิน **[[จำนวนเงิน]]** บาท</p> <p>**ข้อ 2.** สำหรับราคาสินค้าส่วนนี้ผู้ซื้อตกลงชำระให้แก่ผู้ขายภายในวันที่ **[[กำหนดชำระเงิน:Date]]**</p> <p>**ข้อ 3.** หากผู้ขายได้รับเงินแล้ว จะต้องดำเนินการส่งสินค้าภายในเวลา **[[จัดส่งภายใน]]** วัน</p> <p>**ข้อ 4.** หากผู้สัญญาฝ่ายหนึ่งฝ่ายใดเกิดสัญญา ให้อีกฝ่ายหนึ่งมีสิทธิบอกเลิกสัญญาและมีสิทธิเรียกร้องค่าเสียหายจากฝ่ายที่ผิดสัญญาได้ตามความเป็นจริง</p> <p>ลงวันที่ **[[วันที่:Date]]**</p> <p>ลงชื่อ **[[ชื่อผู้ขาย]]** ผู้ขาย</p> <p>ลงชื่อ **[[ชื่อผู้ซื้อ]]** ผู้ซื้อ</p> <p>ลงชื่อ **[[witness]]** พยาน</p>	<div>สัญญาซื้อขายขนม</div> <div>— Please choose from the list —</div> <div>จำนวนสินค้าที่สั่งซื้อ</div> <div>จำนวนเงิน</div> <div>กำหนดชำระเงิน</div> <div>จัดส่งภายใน</div> <div>วันที่</div> <div>ชื่อผู้ขาย</div> <div>ชื่อผู้ซื้อ</div> <div>witness</div>	<div>Download PDF</div> <p>สัญญาซื้อขายขนม ____</p> <p>ข้อ 1. ผู้ขายตกลงขายและผู้ซื้อตกลงซื้อขนมของผู้ขาย จำนวน ____ ชิ้น รวมเป็นเงิน ____ บาท</p> <p>ข้อ 2. สำหรับราคาสินค้าส่วนนี้ผู้ซื้อตกลงชำระให้แก่ผู้ขายภายในวันที่ ____</p> <p>ข้อ 3. หากผู้ขายได้รับเงินแล้ว จะต้องดำเนินการส่งสินค้าภายในเวลา ____ วัน</p> <p>ข้อ 4. หากผู้สัญญาฝ่ายหนึ่งฝ่ายใดเกิดสัญญา ให้อีกฝ่ายหนึ่งมีสิทธิบอกเลิกสัญญาและมีสิทธิเรียกร้องค่าเสียหายจากฝ่ายที่ผิดสัญญาได้ตามความเป็นจริง</p> <p>ลงวันที่ ____</p> <p>ลงชื่อ ____ ผู้ขาย</p> <p>ลงชื่อ ____ ผู้ซื้อ</p> <p>ลงชื่อ ____ พยาน</p> <div>SEND TO BLOCKCHAIN ></div>

3. Alice start filling a form.

Form	Preview
สัญญาซื้อขายขนม — Please choose from the list — จำนวนสินค้าที่สั่งซื้อ จำนวนเงิน กำหนดชำระเงิน จัดส่งภายใน วันที่ ชื่อผู้ขาย ชื่อผู้ซื้อ witness	Download PDF สัญญาซื้อขายขนม ____ ข้อ 1. ผู้ขายตกลงขายและผู้ซื้อตกลงซื้อขนมของผู้ขาย จำนวน ____ ชิ้น รวมเป็นเงิน ____ บาท ข้อ 2. สำหรับราคาสินค้าส่วนนั้นผู้ซื้อตกลงชำระให้แก่ผู้ขายภายในวันที่ ____ ข้อ 3. หากผู้ขายได้รับเงินแล้ว จะต้องดำเนินการส่งสินค้าภายในเวลา ____ วัน ข้อ 4. หากคู่สัญญาฝ่ายหนึ่งฝ่ายใดผิดสัญญา ให้อีกฝ่ายหนึ่งมีสิทธิบอกเลิกสัญญาและมีสิทธิเรียกร้องค่าเสียหายจากฝ่ายที่ผิดสัญญาได้ตามความเป็นจริง ลงวันที่ ____ ลงชื่อ ____ ผู้ขาย ลงชื่อ ____ ผู้ซื้อ ลงชื่อ ____ พยาน SEND TO BLOCKCHAIN

4. This form support many type of input (e.g., date, choices). Final preview of the contract is shown on the right.

Form	Preview
สัญญาซื้อขายขนม หาใช่ 20 400 June 9, 2022 20 June 8, 2022	Download PDF สัญญาซื้อขายขนม หาใช่ ข้อ 1. ผู้ขายตกลงขายและผู้ซื้อตกลงซื้อขนมของผู้ขาย จำนวน 20 ชิ้น รวมเป็นเงิน 400 บาท ข้อ 2. สำหรับราคาสินค้าส่วนนั้นผู้ซื้อตกลงชำระให้แก่ผู้ขายภายในวันที่ June 9, 2022 ข้อ 3. หากผู้ขายได้รับเงินแล้ว จะต้องดำเนินการส่งสินค้าภายในเวลา 20 วัน ข้อ 4. หากคู่สัญญาฝ่ายหนึ่งฝ่ายใดผิดสัญญา ให้อีกฝ่ายหนึ่งมีสิทธิบอกเลิกสัญญาและมีสิทธิเรียกร้องค่าเสียหายจากฝ่ายที่ผิดสัญญาได้ตามความเป็นจริง ลงวันที่ June 8, 2022 ลงชื่อ Alice ผู้ขาย ลงชื่อ Bob ผู้ซื้อ ลงชื่อ Catherine พยาน SEND TO BLOCKCHAIN

5. Once Alice is done creating a contract, she can download it as a PDF.

[Download PDF](#)

6. Alice click "Send to Blockchain" to deploy this contract to the blockchain.

[SEND TO BLOCKCHAIN](#)

7. There are 3 things that Alice need to fill in before sending it to the blockchain,
- The document that she want to store as a hash (ie, pdf file of a contract she created)
 - small detail about this contract as a reminder
 - Recipient ,in this case, Bob ethereum address

Upload file : contract.pdf you downloaded above, or any other document that you want to store as on the blockchain (as a hash for now)

Choose File snack_contract (11).pdf

type some short description about what is this contract about

demo contract

Recipient address

0xFEfA7bea8457ed525F4120579f2dF852234274cC

Before you sign, set your metamask to Ropsten test network and please make sure that you have some Ether

SIGN

8. Click SIGN, Metamask will pop up and ask Alice to sign a transaction , Alice has to pay a small fee, since it change the state of the blockchain. If the transaction is successful, she will see green popup telling her that Contract are successfully deployed.

✔ Contract succesfully deployed on blockchain , check "view deployed contract" tab to see all of your contracts

9. Alice go to "view deployed contracts" tab to see her deployed contract. Since this application has no backend. This page queries contract information from the blockchain directly. She can see that her contract (#0) is successfully deployed, and is in pending status waiting for Bob (0xFE..) to sign it.

press "f5" to refresh the page , expect at least 20 second for the block chain to process transaction)

localhost:3000/view

some | view deployed contracts |

ropsten test network :0x8bd126632b72715929B1FE7DaF1Ea92BD7D8d3B8

Deployed at 0x8bd126632b72715929B1FE7DaF1Ea92BD7D8d3B8

Pending Contract

Contract ID	detail	hash	...to be signed by...
0	demo contract	059f2811b81650c903629449ca76bcc6f62d21c57c30e4d3474c2c97f58d7c39	0xFEfA7bea8457ed525F4120579f2dF852234274cC

Completed Contract

No complete contract

10. The smart contract for this application is currently deployed on Ropsten test network. Click on the link on the top of the page to view this smart contract on Etherscan (code and all transaction history included)

Deployed at 0x8bd126632b72715929B1FE7DaF1Ea92BD7D8d3B8

11. On Bob 's side, he can see a pending contract that ask for his signature.

[Home](#) | [view deployed contracts](#) |

ropsten test network :0x8bd126632b72715929B1FE7DaF1Ea92BD7D8d3B8

Deployed at [0x8bd126632b72715929B1FE7DaF1Ea92BD7D8d3B8](#)

Pending Contract

Contract ID	detail	hash	...to be signed by...
0	demo contract	059f2811b81650c903629449ca76bcc6f62d21c57c30e4d3474c2c97f58d7c39	<input type="button" value="sign"/>

Completed Contract

No complete contract

12. Once Bob sign the contract, this contract will be mark as completed (Bob has to pay transaction fee to sign and push change to blockchain.)

Deployed at [0x8bd126632b72715929B1FE7DaF1Ea92BD7D8d3B8](#)

Pending Contract

No pending Contract

Completed Contract

Contract ID	detail	Contract Creator	Signed By	hash	signed Date
0	demo contract	0xB1d1aE061e066AE70E2c794938a619fE7FBFA4	0xFEF1A7bea8457ed525F4120579f2dF852234274cC	059f2811b81650c903629449ca76bcc6f62d21c57c30e4d3474c2c97f58d7c39	Tue Jun 28 2022 00:34:04 GMT+0700 (Indochina Time)

Note:

This web application does not ask any user personal information, no user/password, no cookies or any form of token is needed. It has no backend or cloud storage to store anything. All data are stored and read directly from the blockchain. In this demo, Alice can send Bob a contract's pdf file via an email (or by any other means). Bob can download it and check if its hash match with the one Alice deployed on blockchain. This method is secured.

In the next update, i plan to get rid of the "**Alice have to send file to Bob cause Blockchain is too expensive to store PDF**" part. May be we can store this pdf on some cloud or some decentralized server like IPFS automatically, so the user does not have to manually send file to each other.