What I will be going over

- What a Smart Contract is
- The uses of a Smart Contract
- The difference between a Call and a Send Transaction
- The difference between a EOA and a Contract Account
- Why we should not store a large amount of data on the Blockchain

Why are Smart Contracts Important?

- Eliminates the need to to trust
- "I will **X** if **Y**"
- Examples:
  - I will **give you the deed** if you **buy at the listed price**
  - I will **notarize this document** if you **provide the info**
  - I will **record your vote** if you **validate your identity**
  - I will **give you the winnings** if the **Toronto Raptors win**

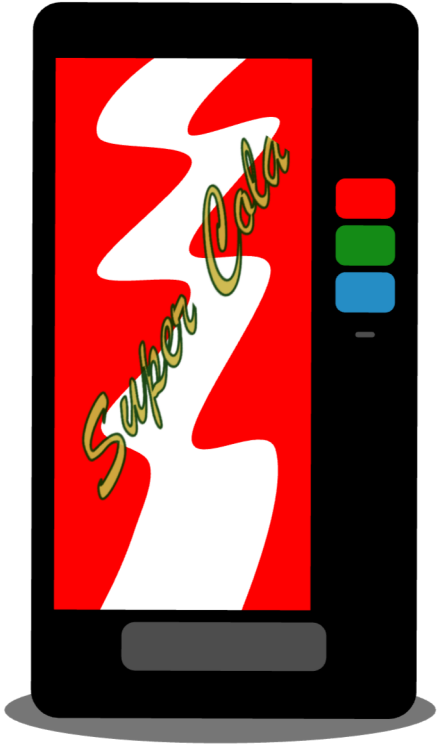
What is a Smart Contract?

“A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises.”
- Nick Szabo

What is a Smart Contract?

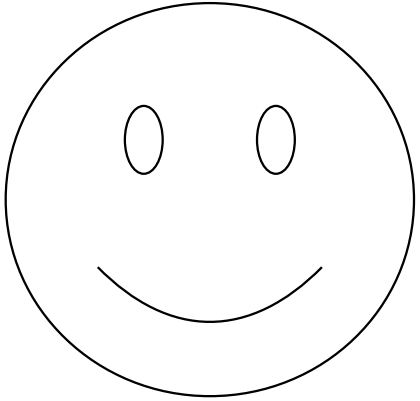
“A canonical real-life example, which we might consider to be the primitive ancestor of smart contracts, is the humble vending machine”
- Nick Szabo

What is a Vending Machine?

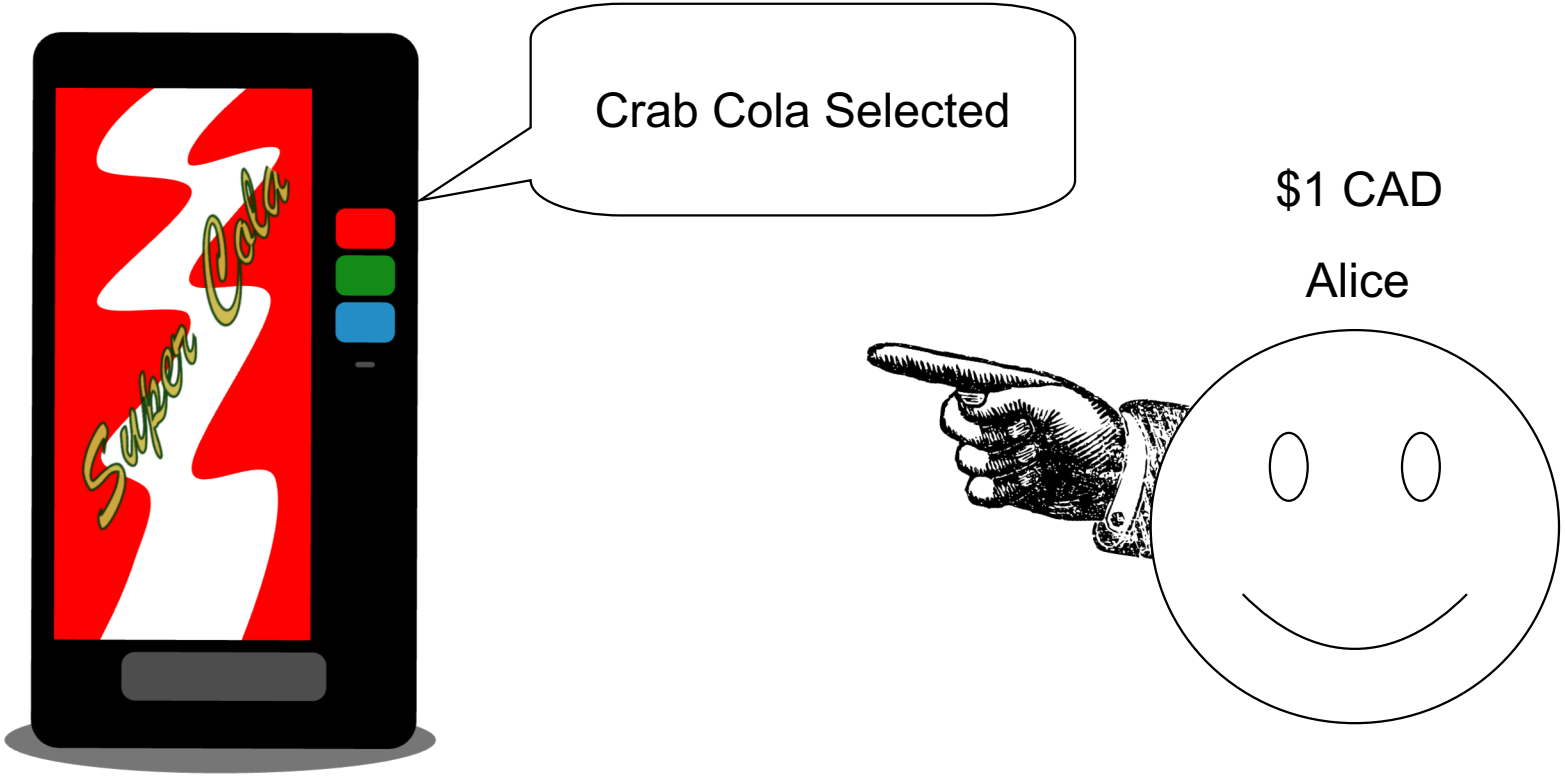


$1 CAD

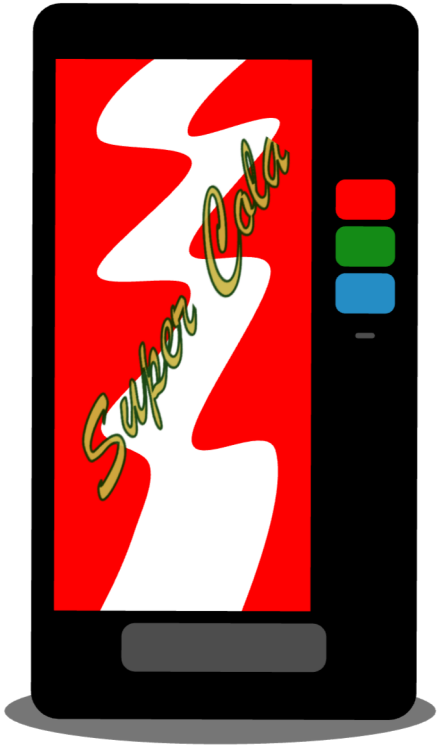
Alice

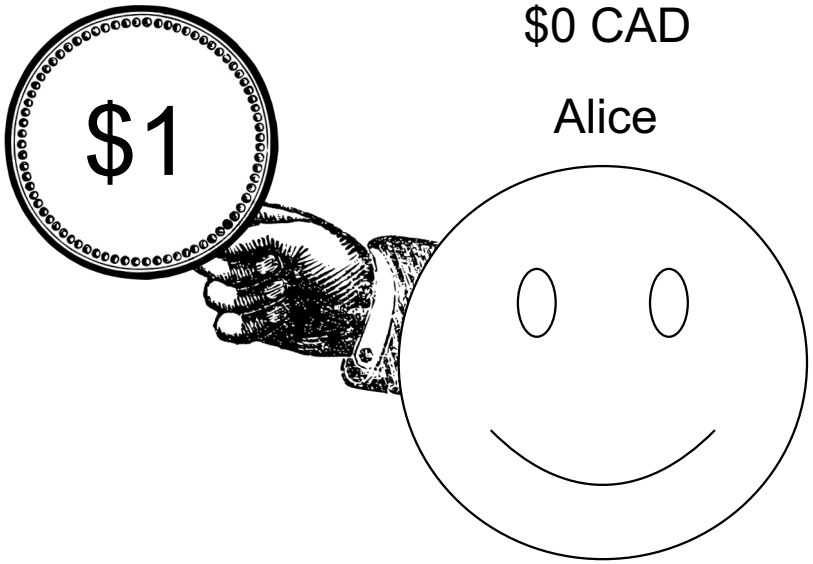


What is a Vending Machine?

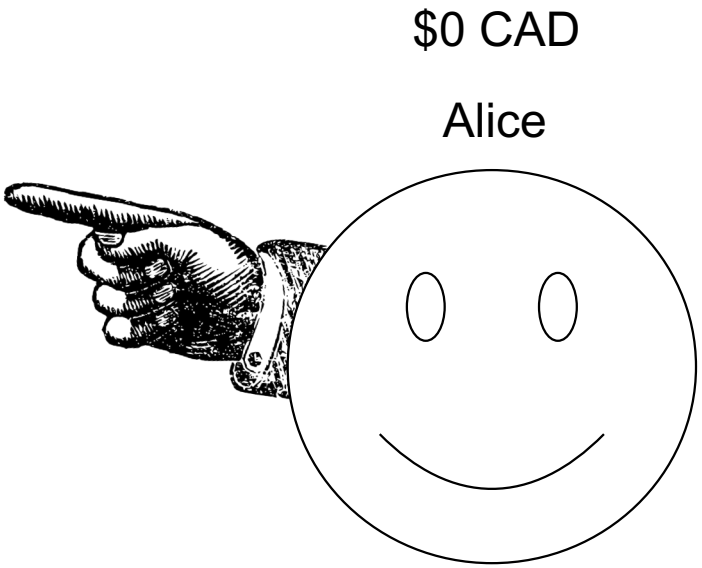


What is a Vending Machine?





What is a Vending Machine?



What is a Vending Machine?

- 1) Alice selects an item
- 2) Alice puts money into the machine
- 3) Crab Cola is dispensed

What is a Vending Machine Contract?

- 1) See all of the drink tokens available
- 2) Send a Transaction to the Smart Contract
- 3) Smart Contract sends back the Crab Cola Token

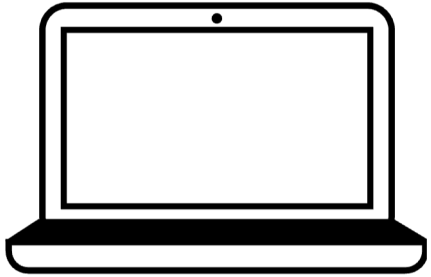
Vending Machine Contract in Action

Vending Machine Contract

0xe6a…

1 ETH

You – 0x6d7...



Contract Call in Action

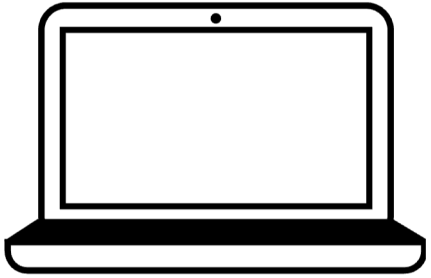
Vending Machine Contract

0xe6a…

Get Menu

1 ETH

You – 0x6d7...



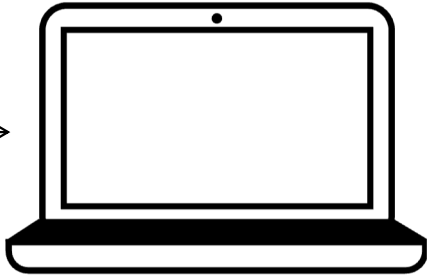
Contract Call in Action

Vending Machine Contract

0xe6a…

1 ETH

You – 0x6d7...



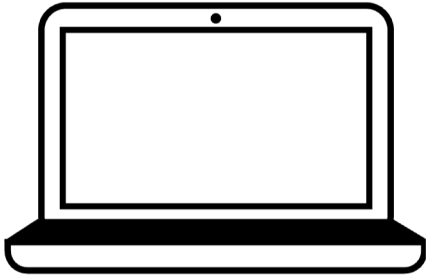
Sending a Transaction to a Contract

Vending Machine Contract

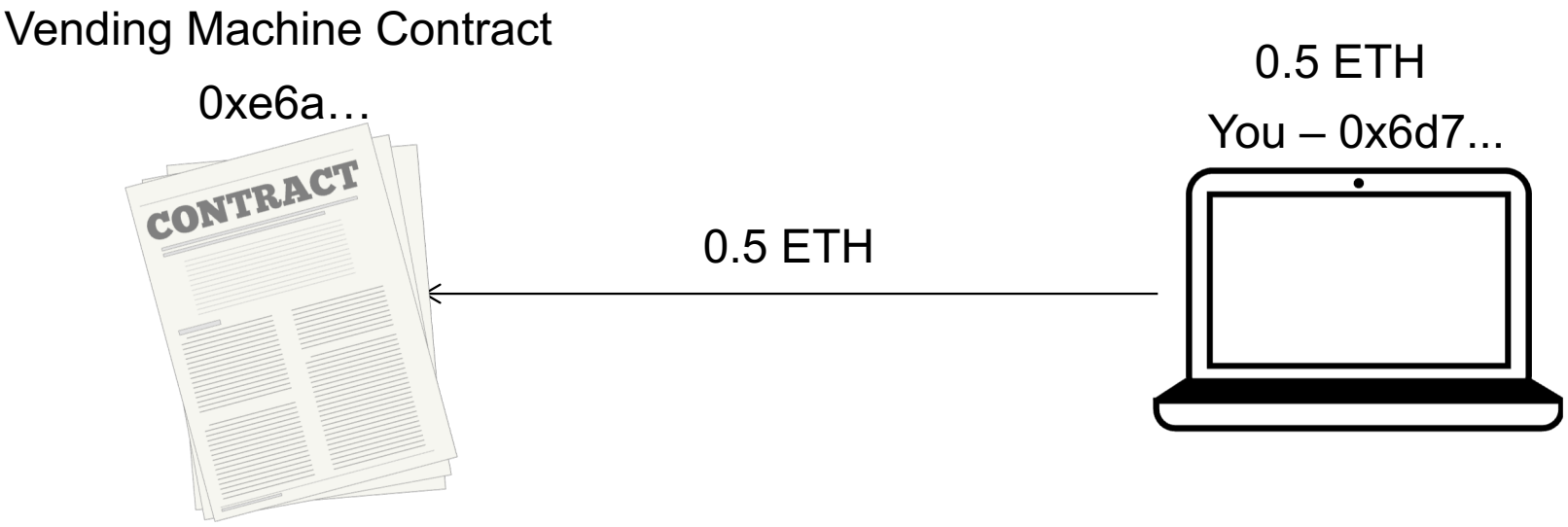
0xe6a…

1 ETH

You – 0x6d7...

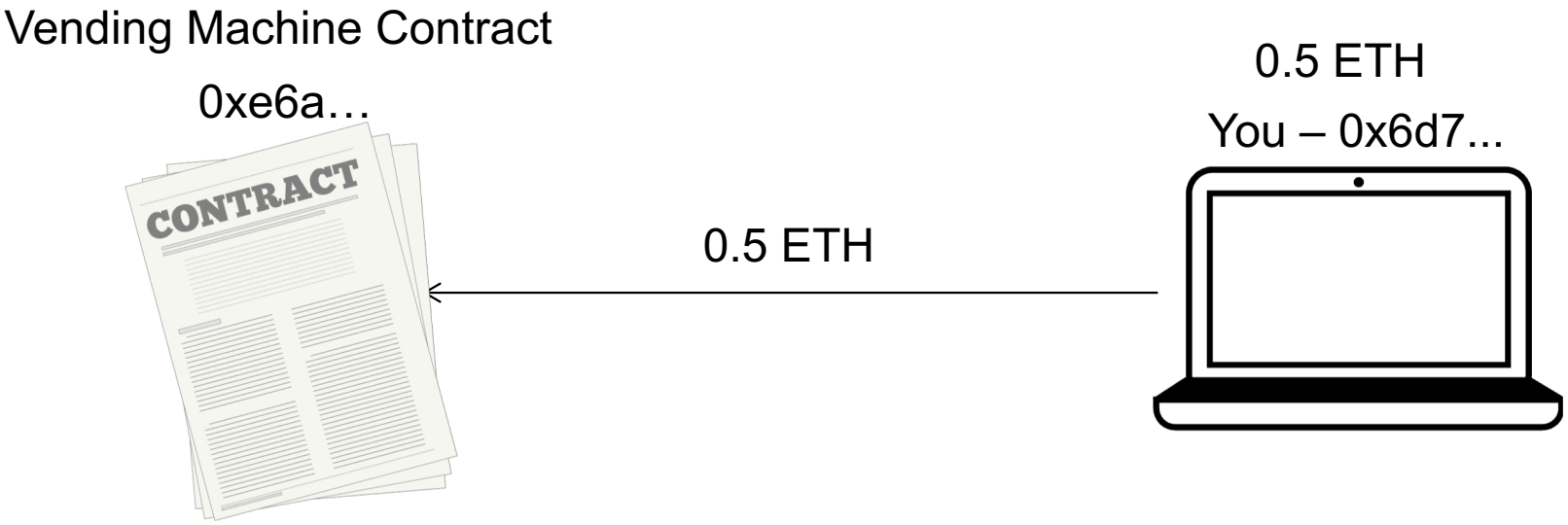


Sending a Transaction to a Contract



Sending a Transaction to a Contract

40,000 GAS (21,000 + 19,000) * 100 Gwei/GAS = **0.004 ETH**



Sending a Transaction to a Contract

40,000 GAS (21,000 + 19,000) * 100 Gwei/GAS = **0.004 ETH**

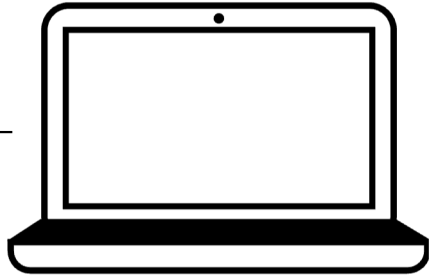
Vending Machine Contract

0xe6a…

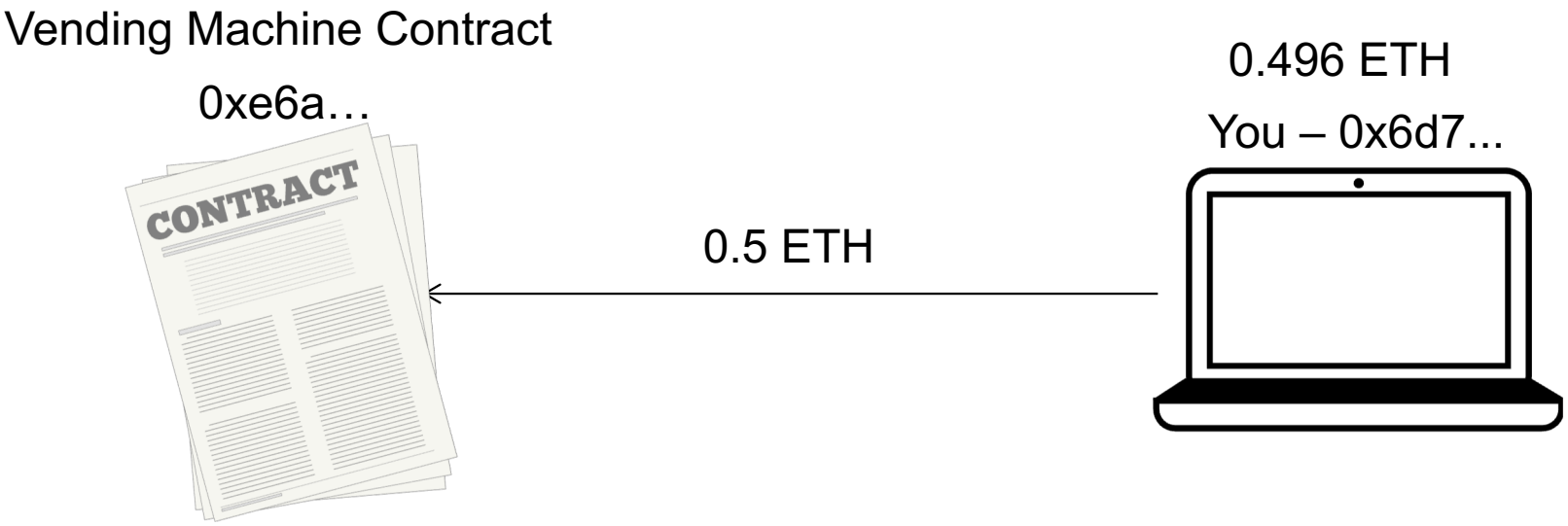
0.5 ETH

0.5 ETH - 0.004 ETH

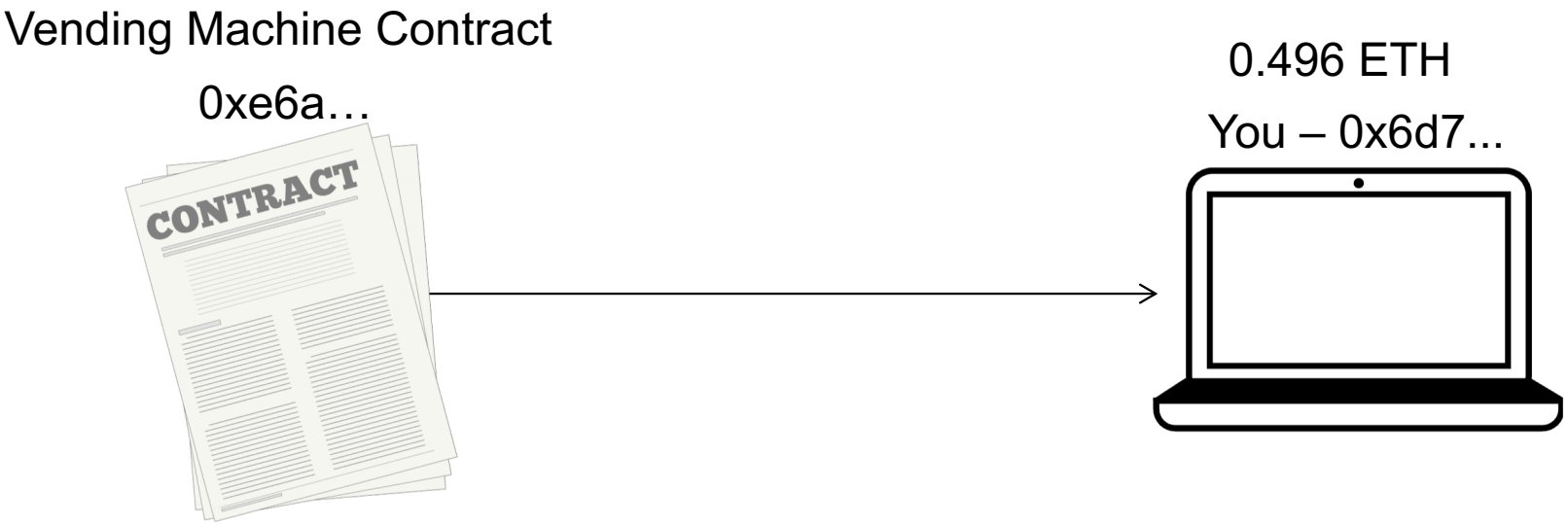
You – 0x6d7...



Sending a Transaction to a Contract



Sending a Transaction to a Contract



Sending a Transaction to a Contract

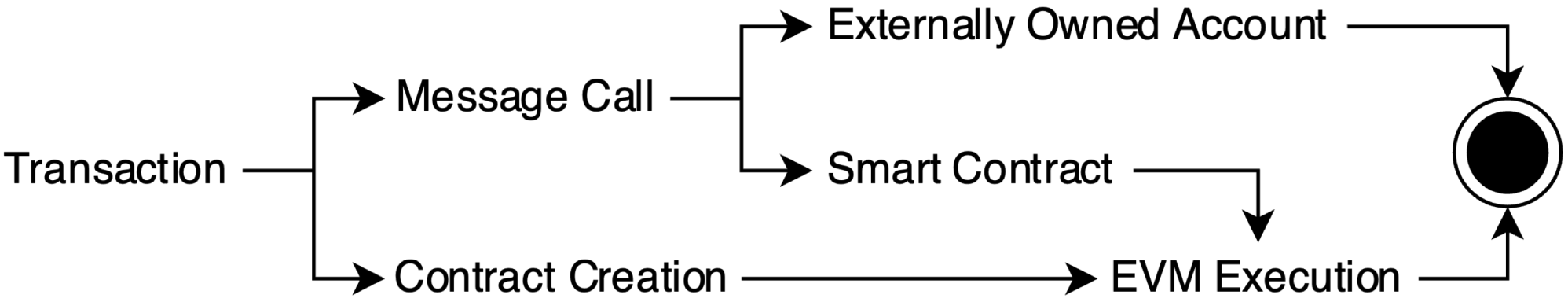
- Costs GAS to send the initial Transaction + every operation
  - External Account → Node → Ethereum Blockchain Network
- Processing is done by **ALL** full nodes in the network
  - Processing is done “inside” of the Ethereum Network
- Changes the state of the Blockchain
- Returns the Transaction Hash (Receipt)

Send Disambiguation

- Web3js – web3.eth.sendTransaction()
- Solidity - <address>.send()

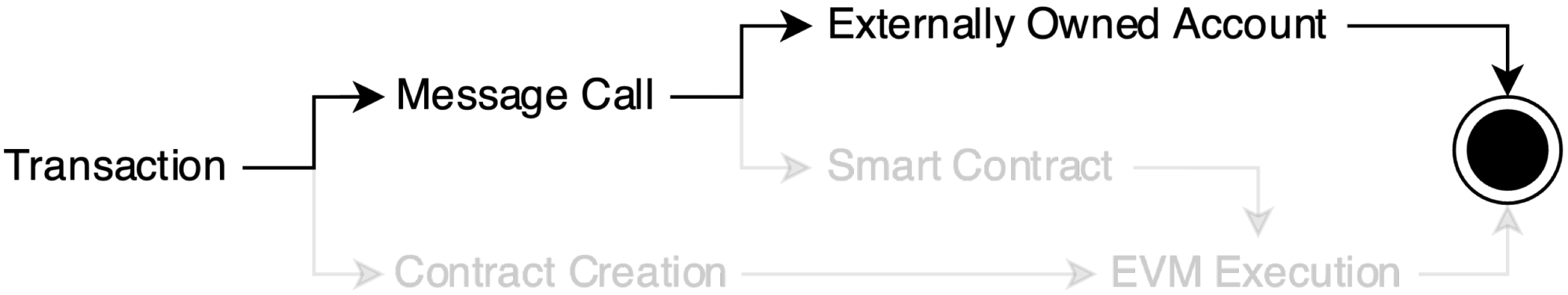
Process of Sending a Transaction

***** Runs on ALL full nodes in the Network *****



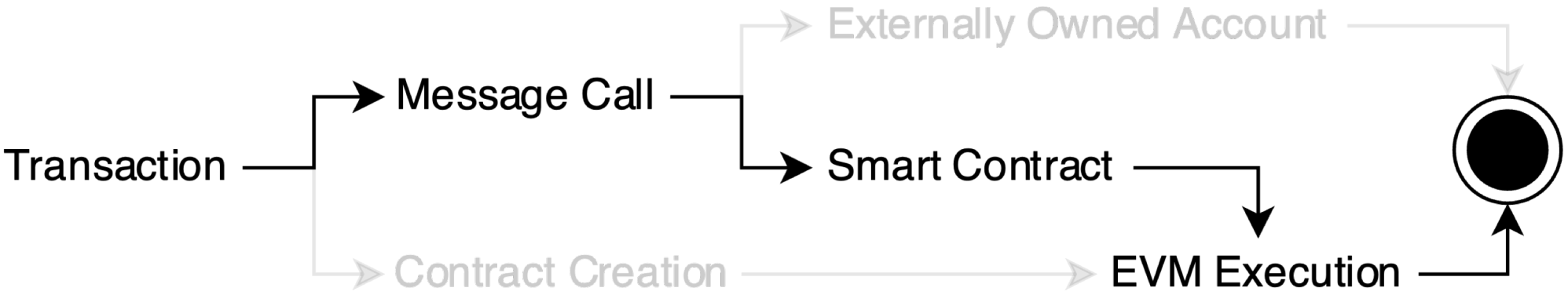
Process of Sending a Transaction

***** Runs on ALL full nodes in the Network *****



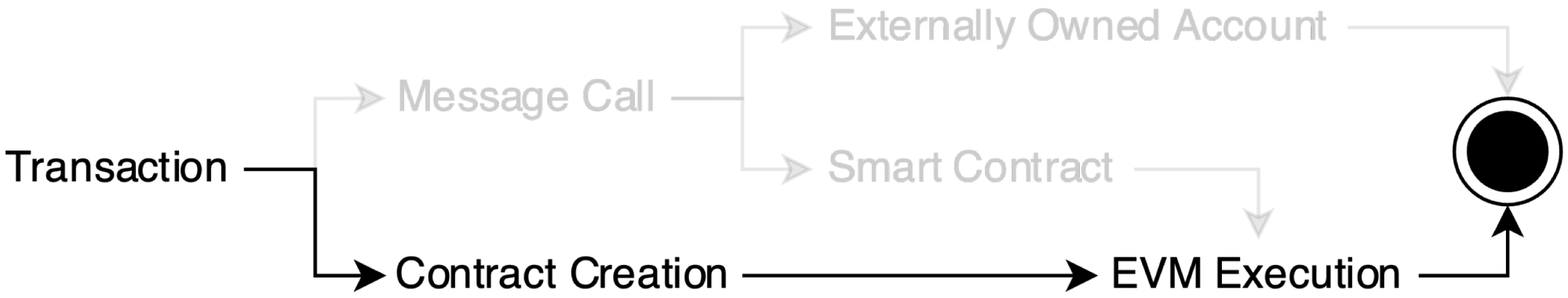
Process of Sending a Transaction

***** Runs on ALL full nodes in the Network *****



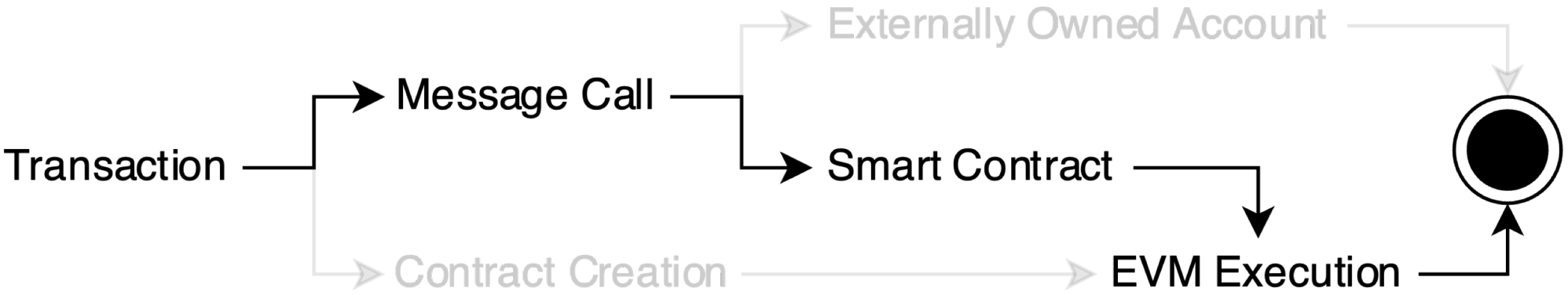
Process of Sending a Transaction

***** Runs on ALL full nodes in the Network *****



Process of Sending a Transaction

***** Runs on ALL full nodes in the Network *****



How does a Transaction look like in Web3.js?

- web3.eth.sendTransaction("0xabc…" {DATA})
- OR
- web3.eth.Contract.functionName().send()
- OR
- web3.eth.Contract.buyToken("CRAB").send()

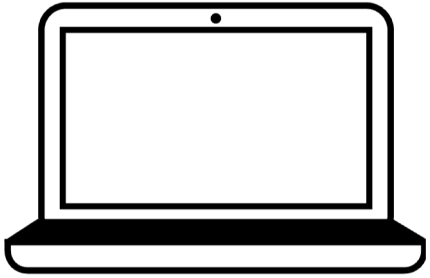
Sending a Transaction to a Contract

Vending Machine Contract

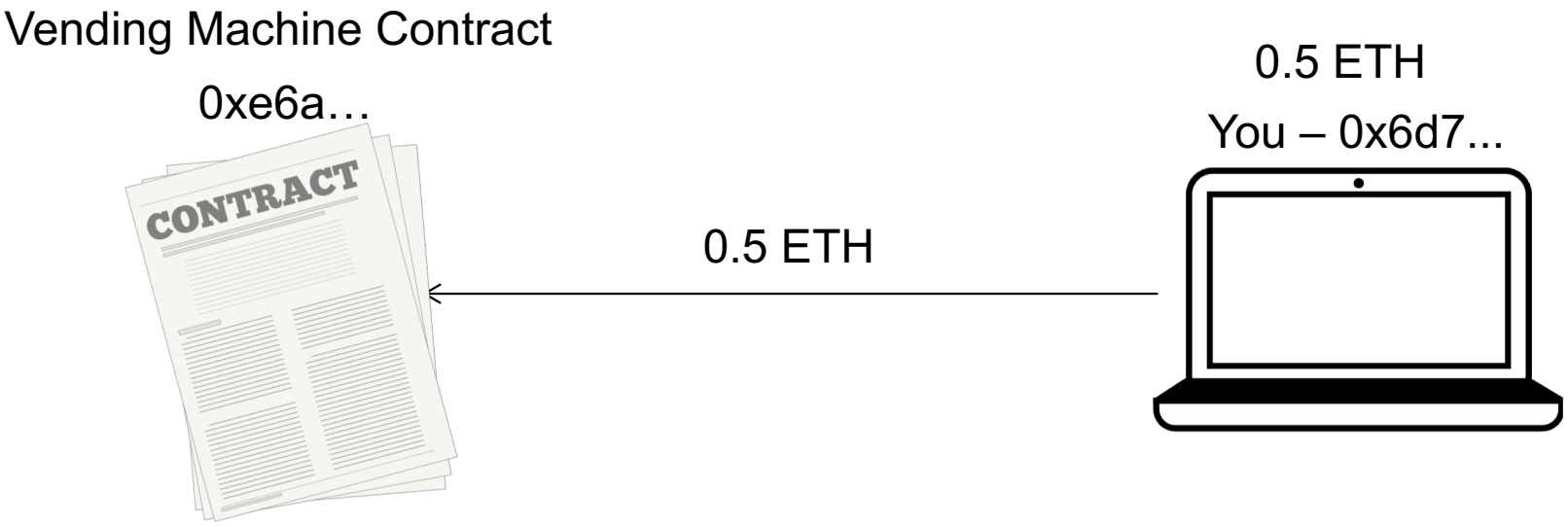
0xe6a…

1 ETH

You – 0x6d7...

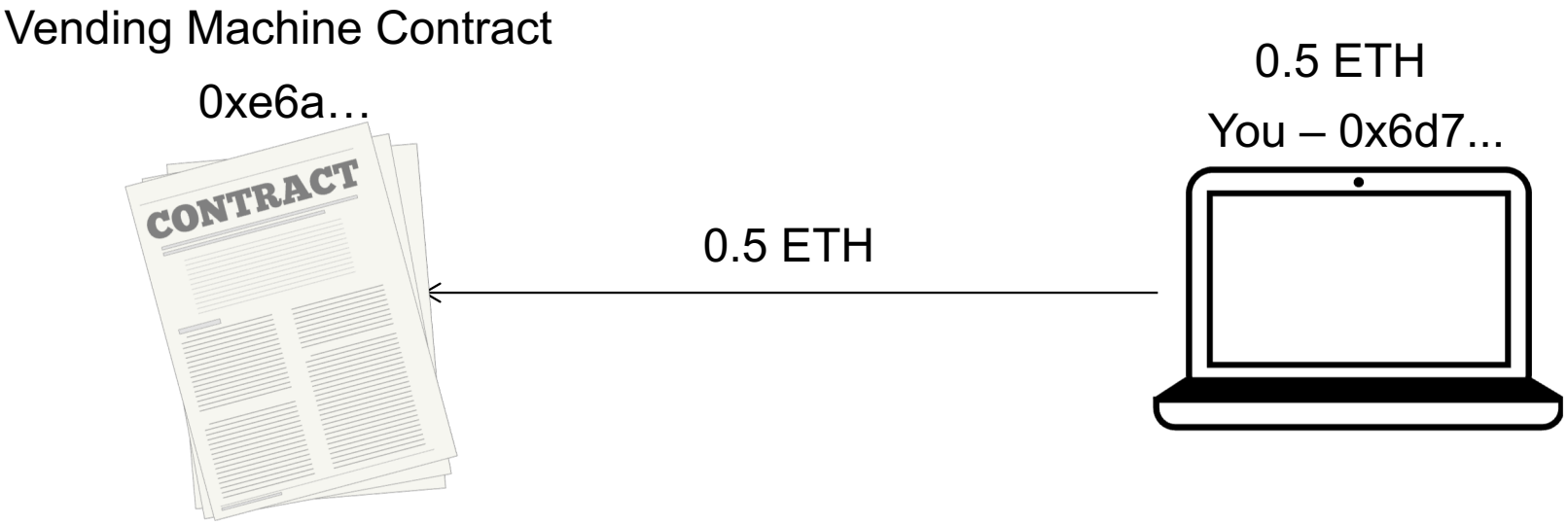


Sending a Transaction to a Contract



Sending a Transaction to a Contract

40,000 GAS (21,000 + 19,000) * 100 Gwei/GAS = **0.004 ETH**



Sending a Transaction to a Contract

40,000 GAS (21,000 + 19,000) * 100 Gwei/GAS = **0.004 ETH**

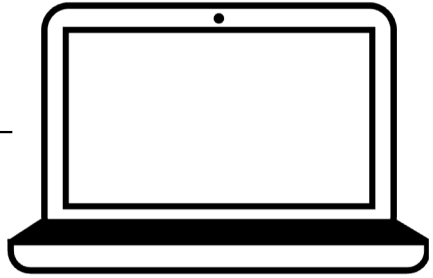
Vending Machine Contract

0xe6a…

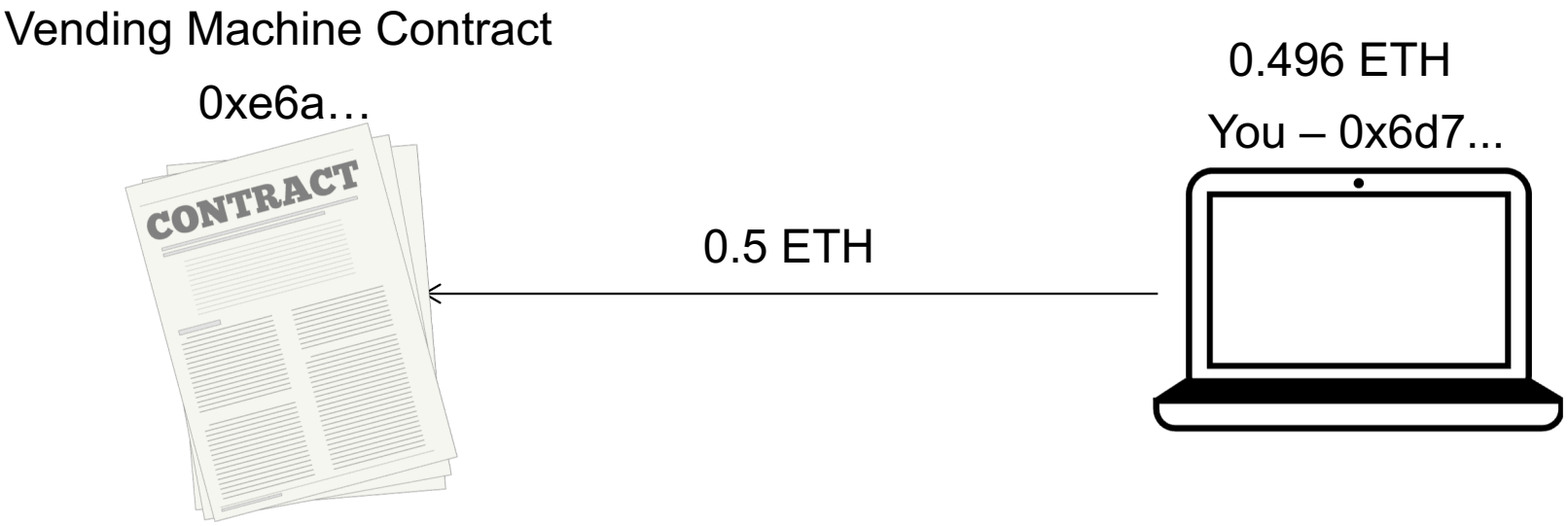
0.5 ETH

0.5 ETH - 0.004 ETH

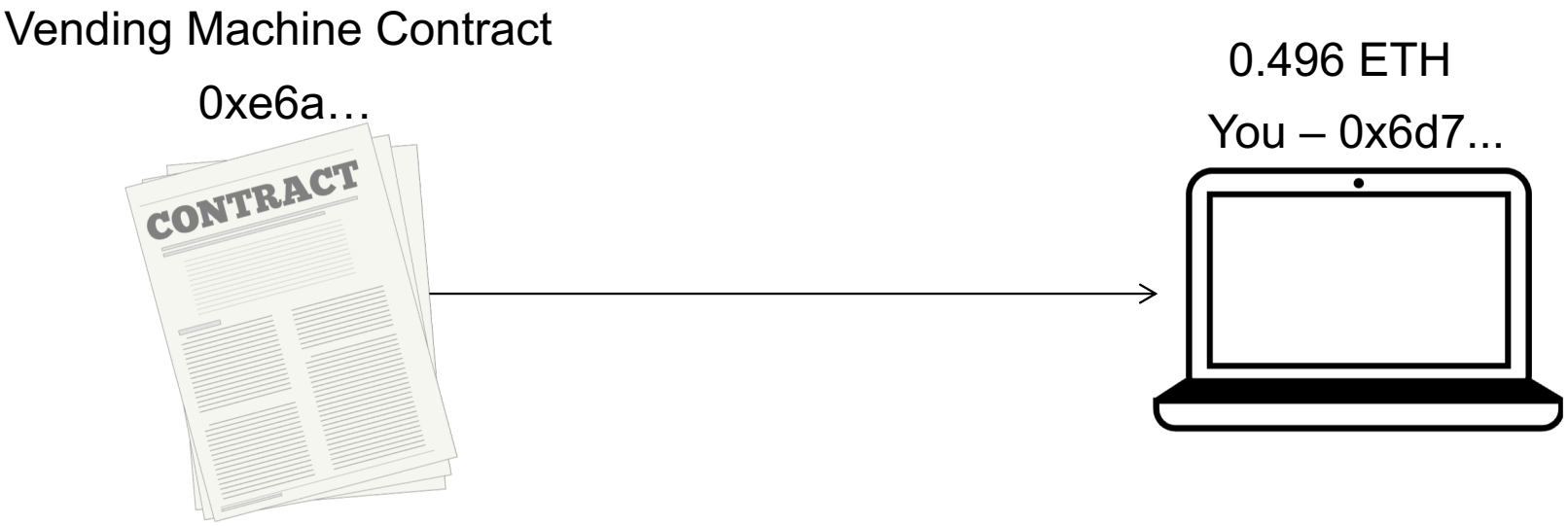
You – 0x6d7...



Sending a Transaction to a Contract



Sending a Transaction to a Contract



Example of a Successful Transaction

Overview | Internal Txns | State

[This is a Ropsten **Testnet** transaction only]

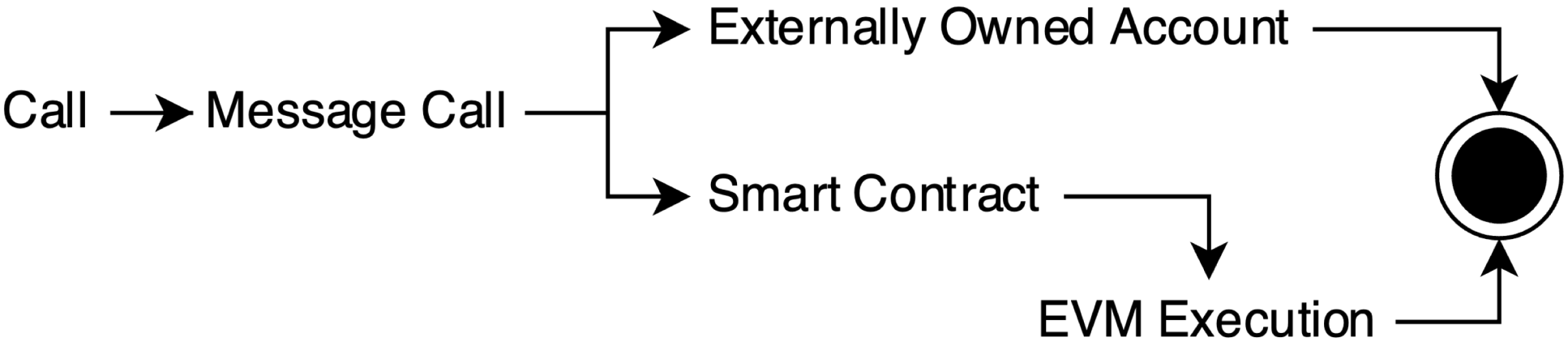
Transaction Hash:	0x44aa5f9c1ed6871766b74cedce20ac197cfe5efc8281ba58ee524ad87b901553
Status:	Success
Block:	8982144 418712 Block Confirmations
Timestamp:	65 days 3 hrs ago (Oct-31-2020 10:05:09 PM +UTC)
From:	0xb7a678a9a6c3623556ff24bb9179ec82765d7a25
To:	Contract 0xec4b315c1c1c429b6747ffb8bbd16cb1eaaa8ff8 L TRANSFER 0.25 Ether From 0xec4b315c1c1c429b6747ffb... To → 0x60a5d33967745d565b3110...
Value:	0.25 Ether ($0.00)
Transaction Fee:	0.00059197718834 Ether ($0.000000)
Gas Price:	0.000000010937627041 Ether (10.937627041 Gwei)
Gas Limit:	84,564
Gas Used by Transaction:	54,123 (64%)
Nonce Position	119 10

Calling a Smart Contract

- Costs no GAS
  - External Account → Node → Local Node Blockchain
- Processing is done on the node
  - Processing is done “outside” of the Ethereum Network
- Does **NOT** change the state of the Blockchain
- Returns the actual value

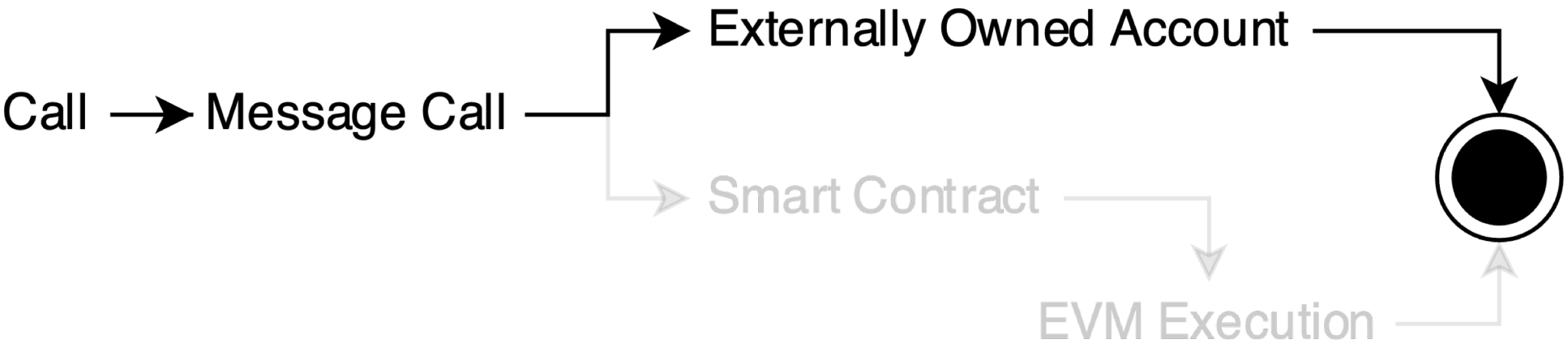
Process of Calling

***** Runs on ONE Node *****



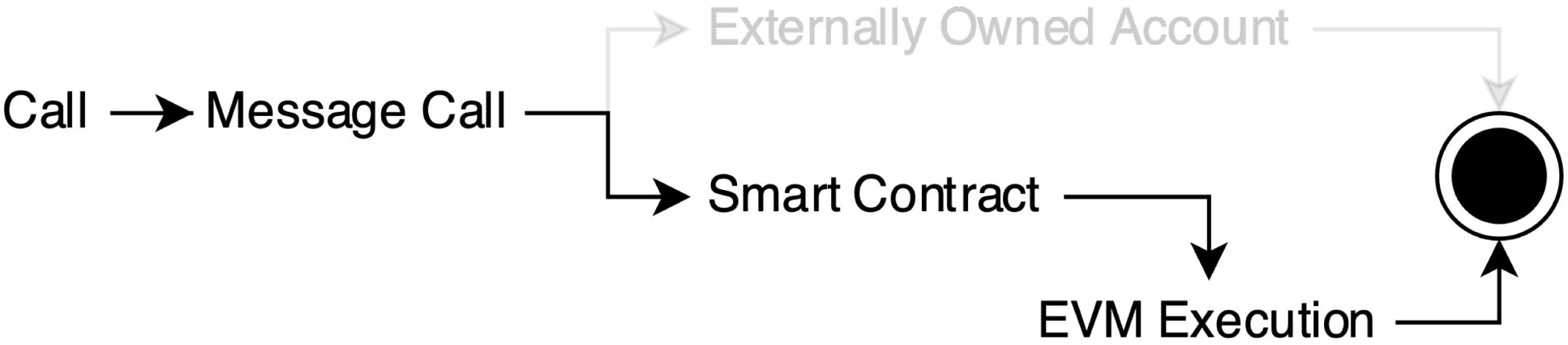
Process of Calling an External Account

***** Runs on ONE Node *****



Process of Calling a Smart Contract

***** Runs on ONE Node *****



How does a Call look like in Web3.js?

- web3.eth.call({DATA});
- OR
- web3.eth.Contract.functionName().call()
- OR
- web3.eth.Contract.getMenu().call()

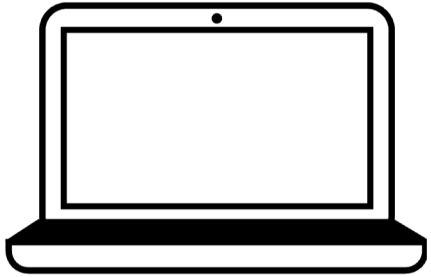
Vending Machine Contract in Action

Vending Machine Contract

0xe6a…

1 ETH

You – 0x6d7...



Vending Machine Contract in Action

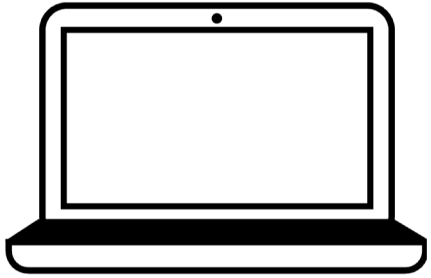
Vending Machine Contract

0xe6a…

Get Menu

1 ETH

You – 0x6d7...



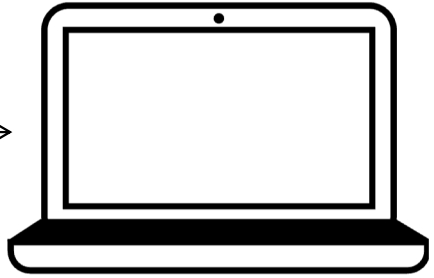
Vending Machine Contract in Action

Vending Machine Contract

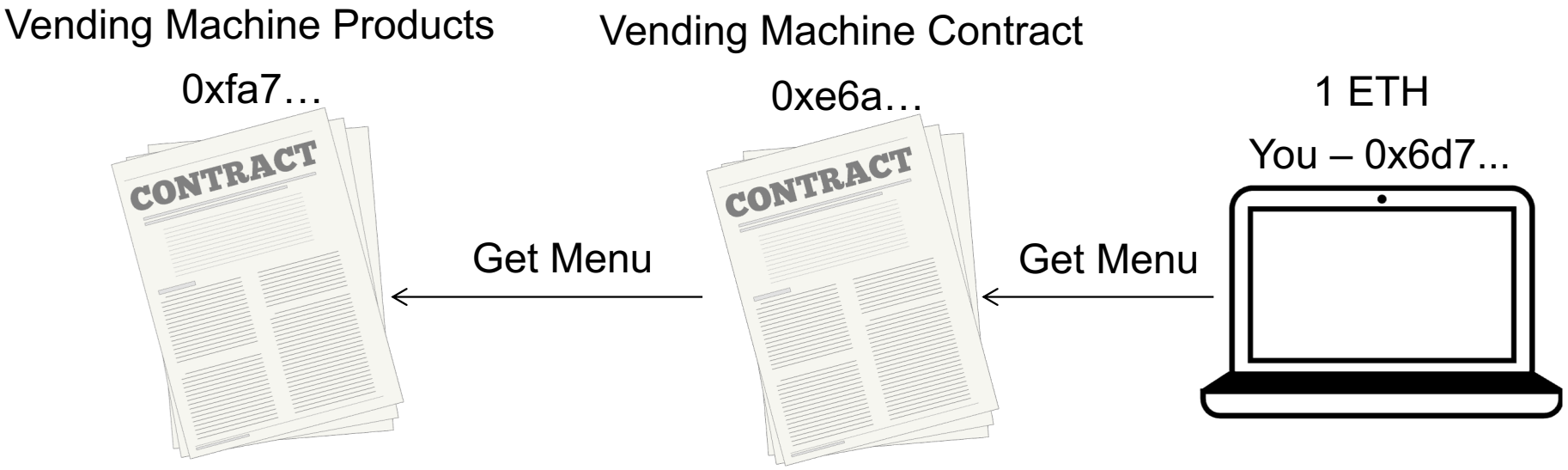
0xe6a…

1 ETH

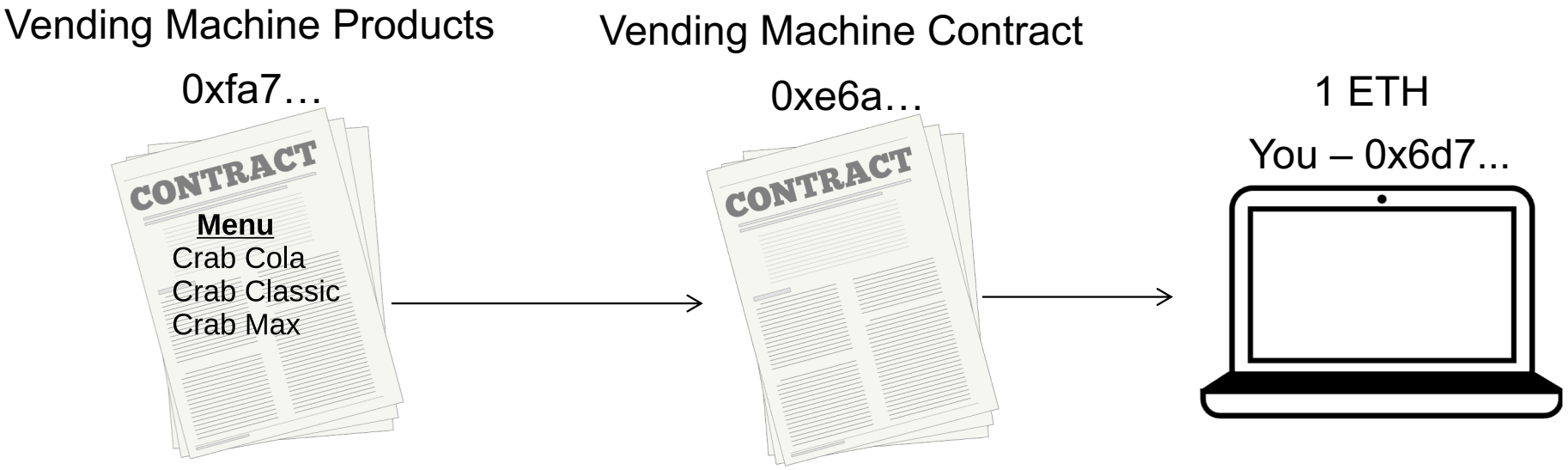
You – 0x6d7...



Vending Machine Contracts in Action

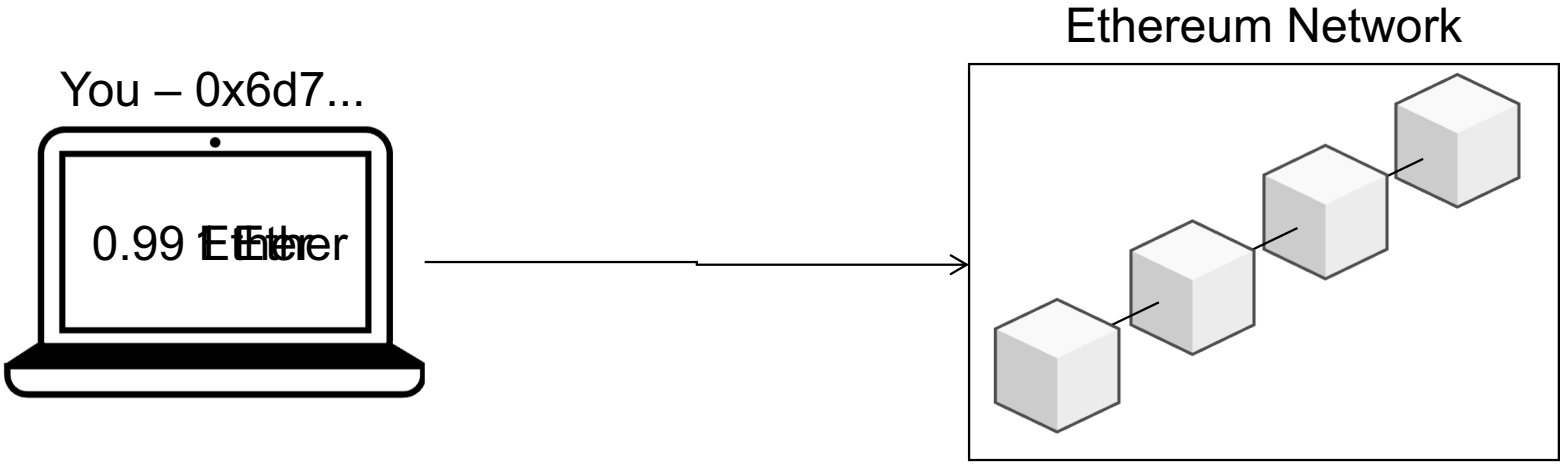


Vending Machine Contracts in Action

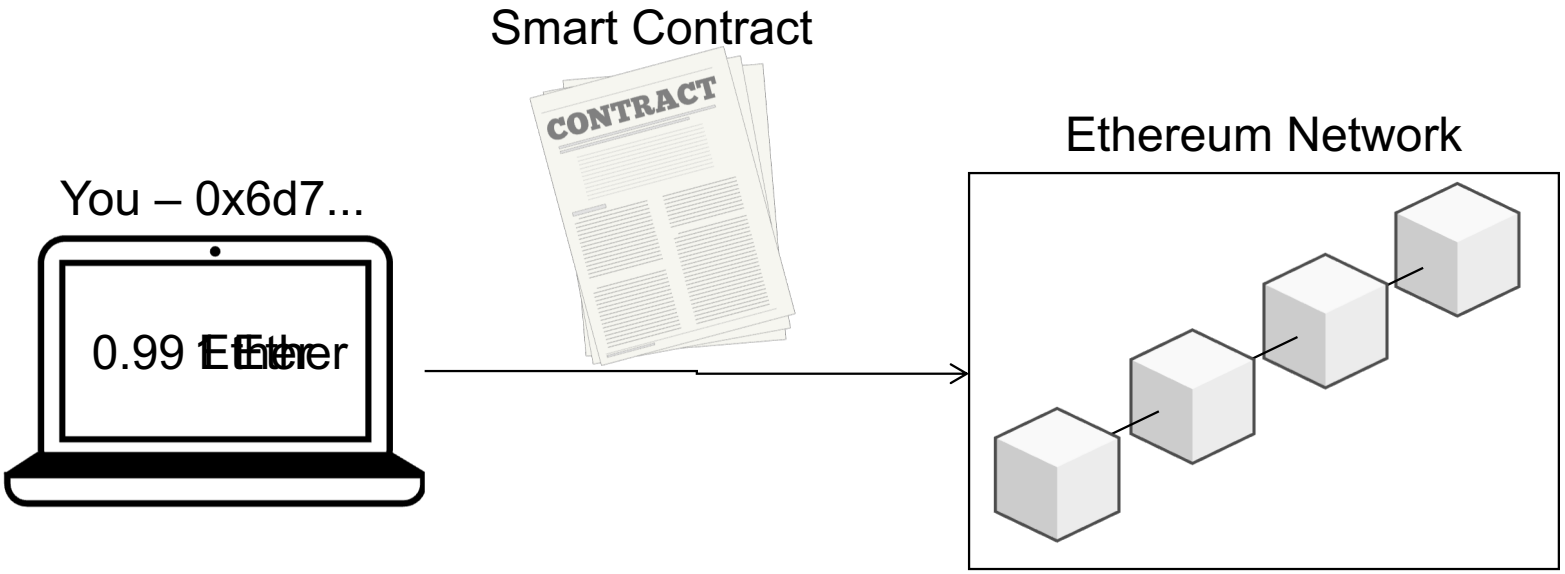


Let’s Deploy a Smart Contract!

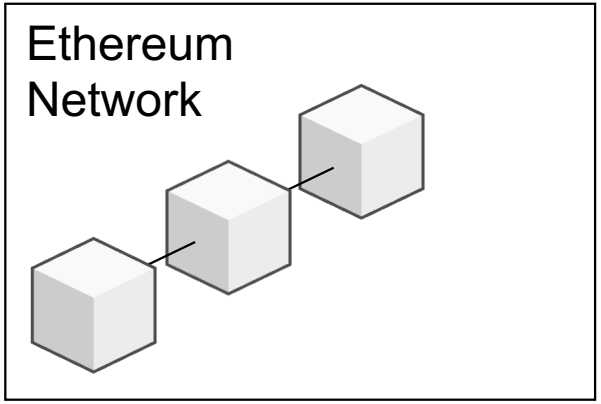
How a Transaction works

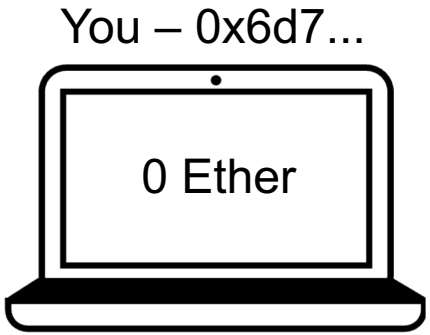


How a Transaction works

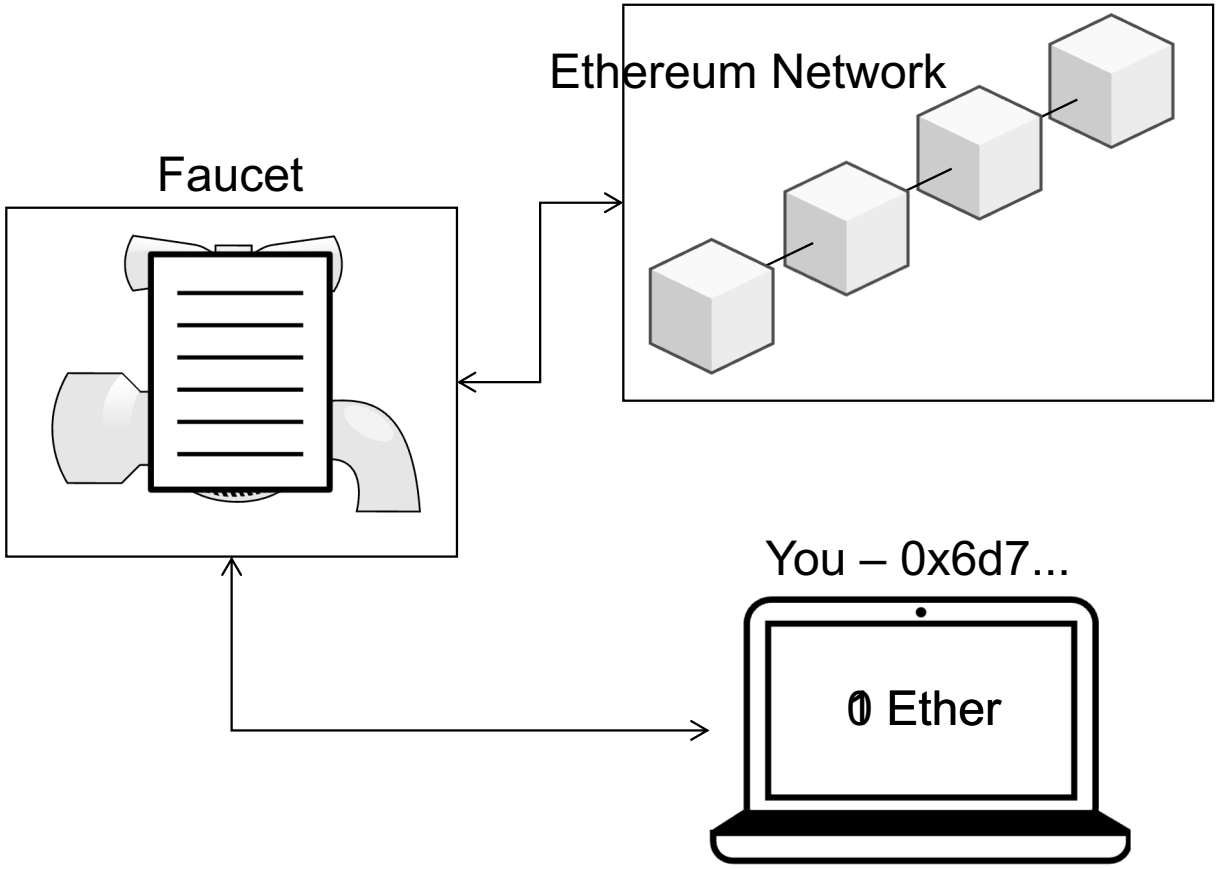


How to get test Ether

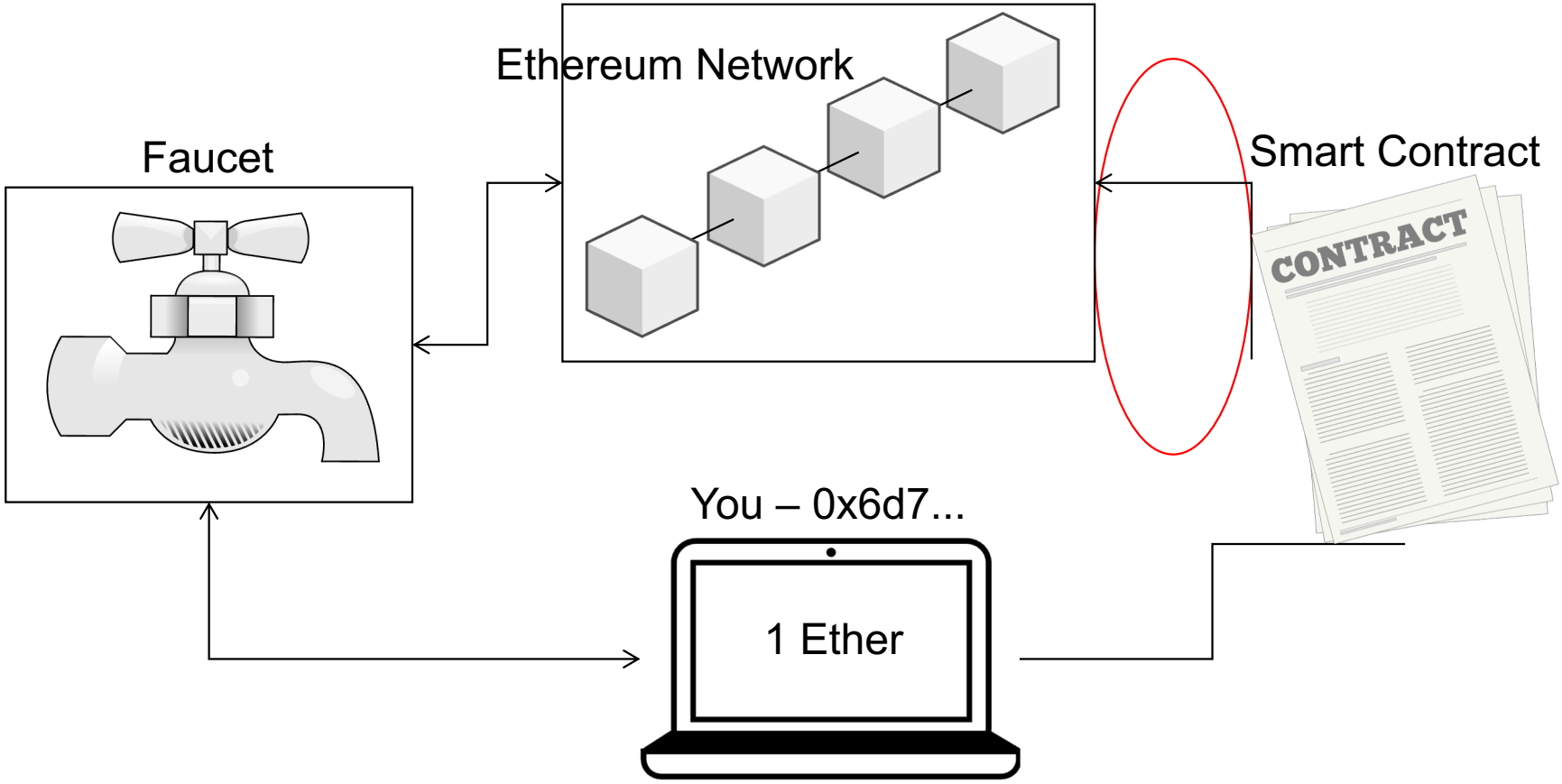




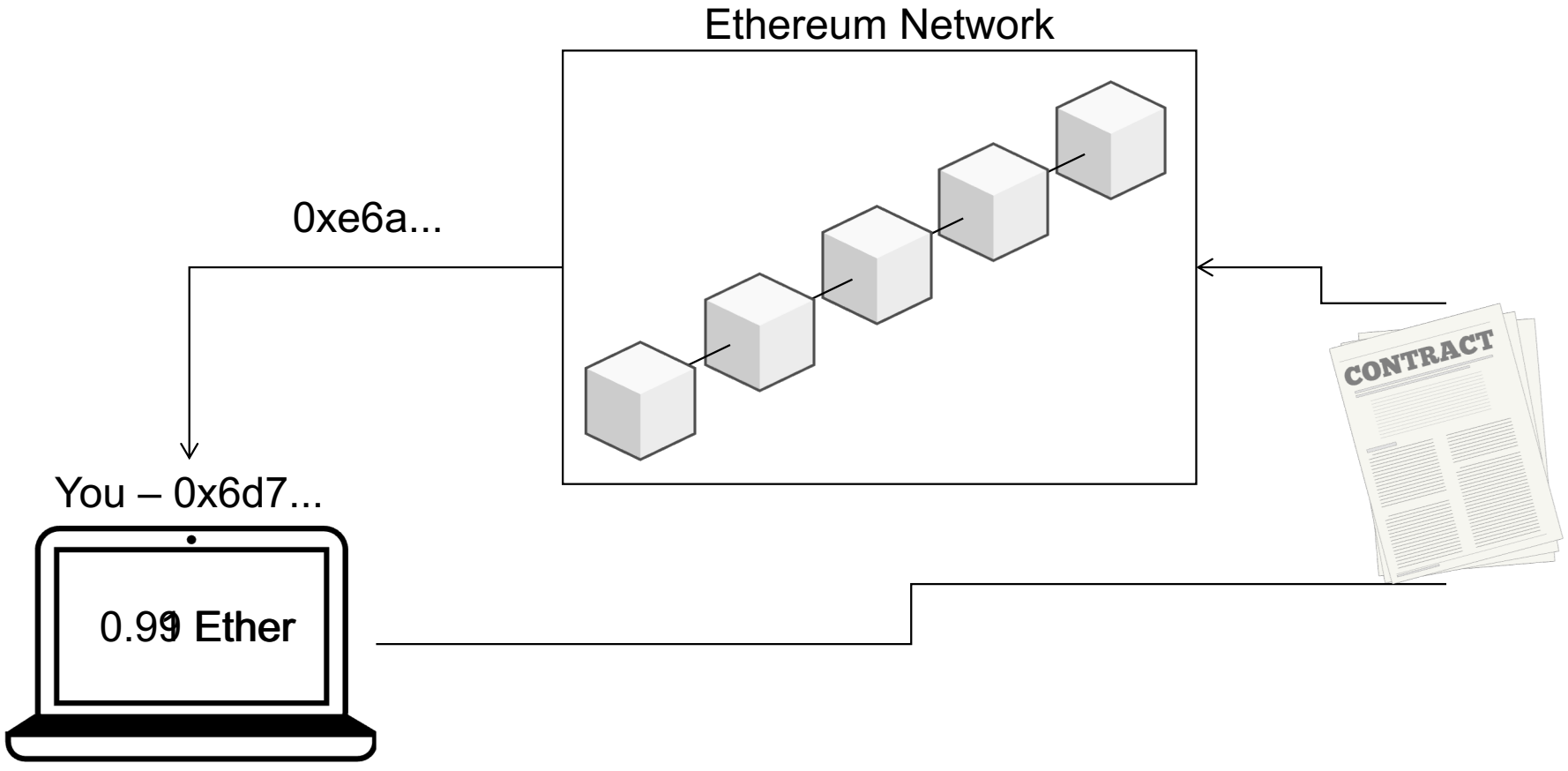
How to get test Ether



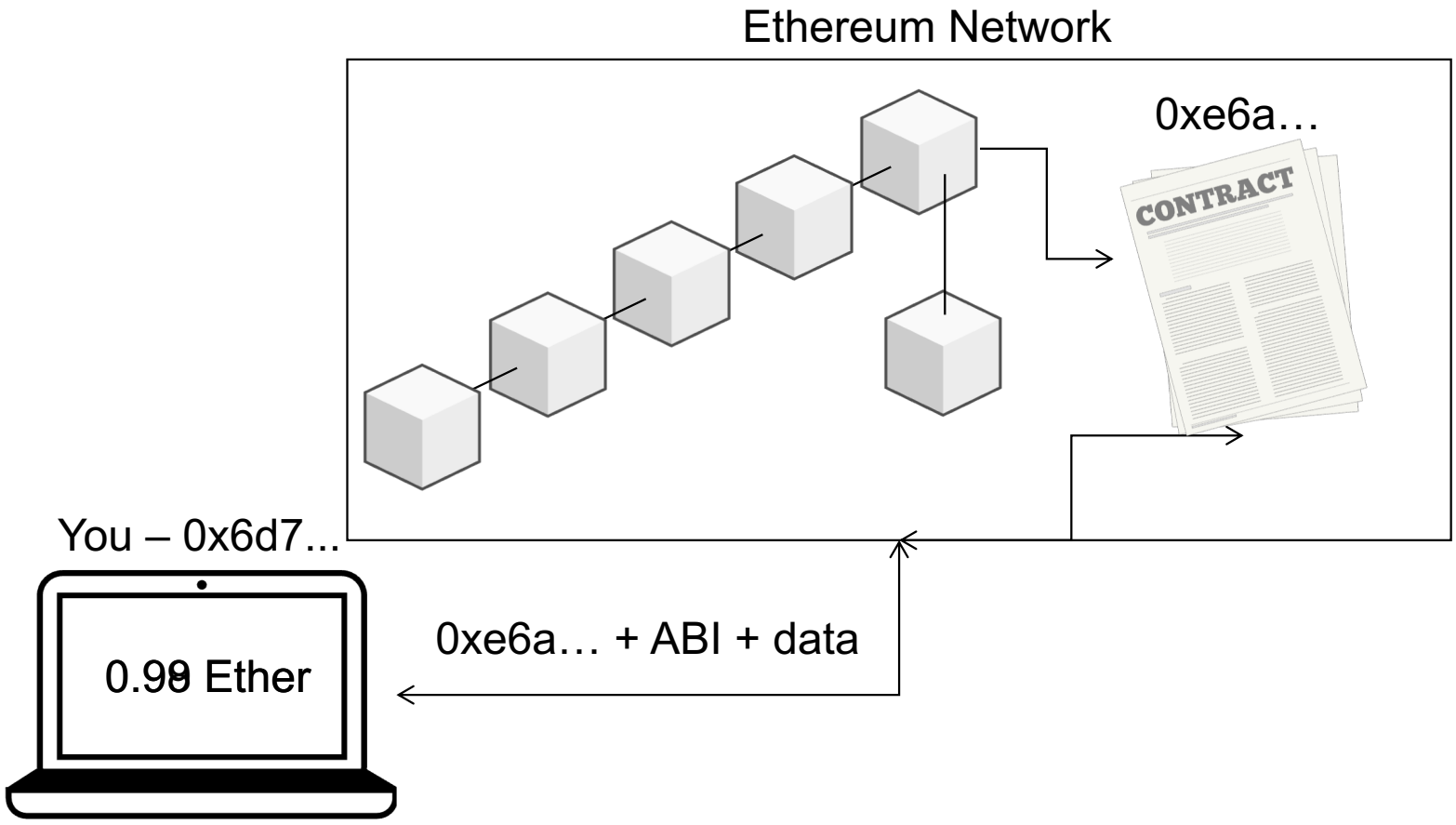
How to get test Ether



Using Transactions to make a Smart Contract



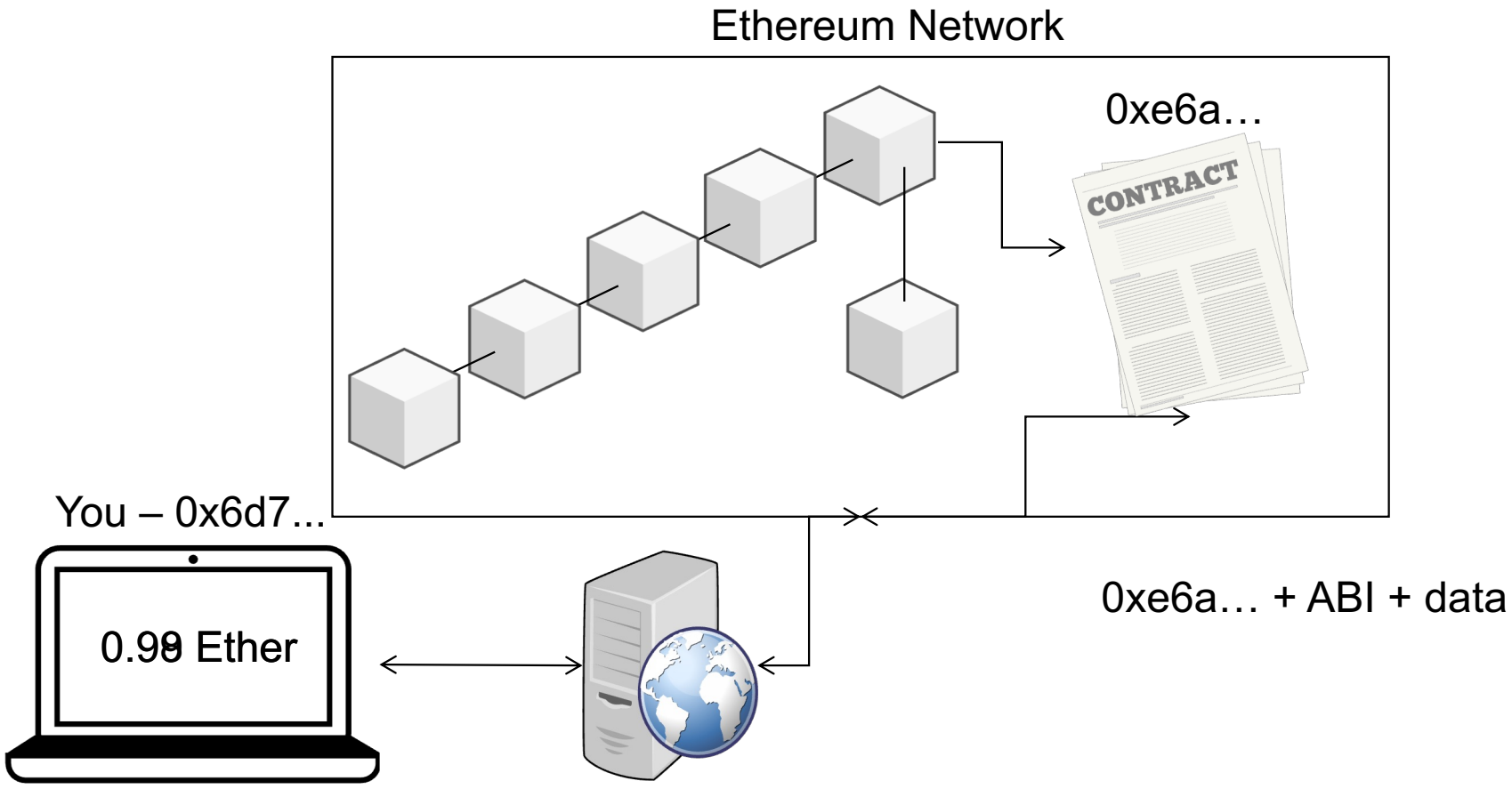
Sending a Transaction to a Smart Contract



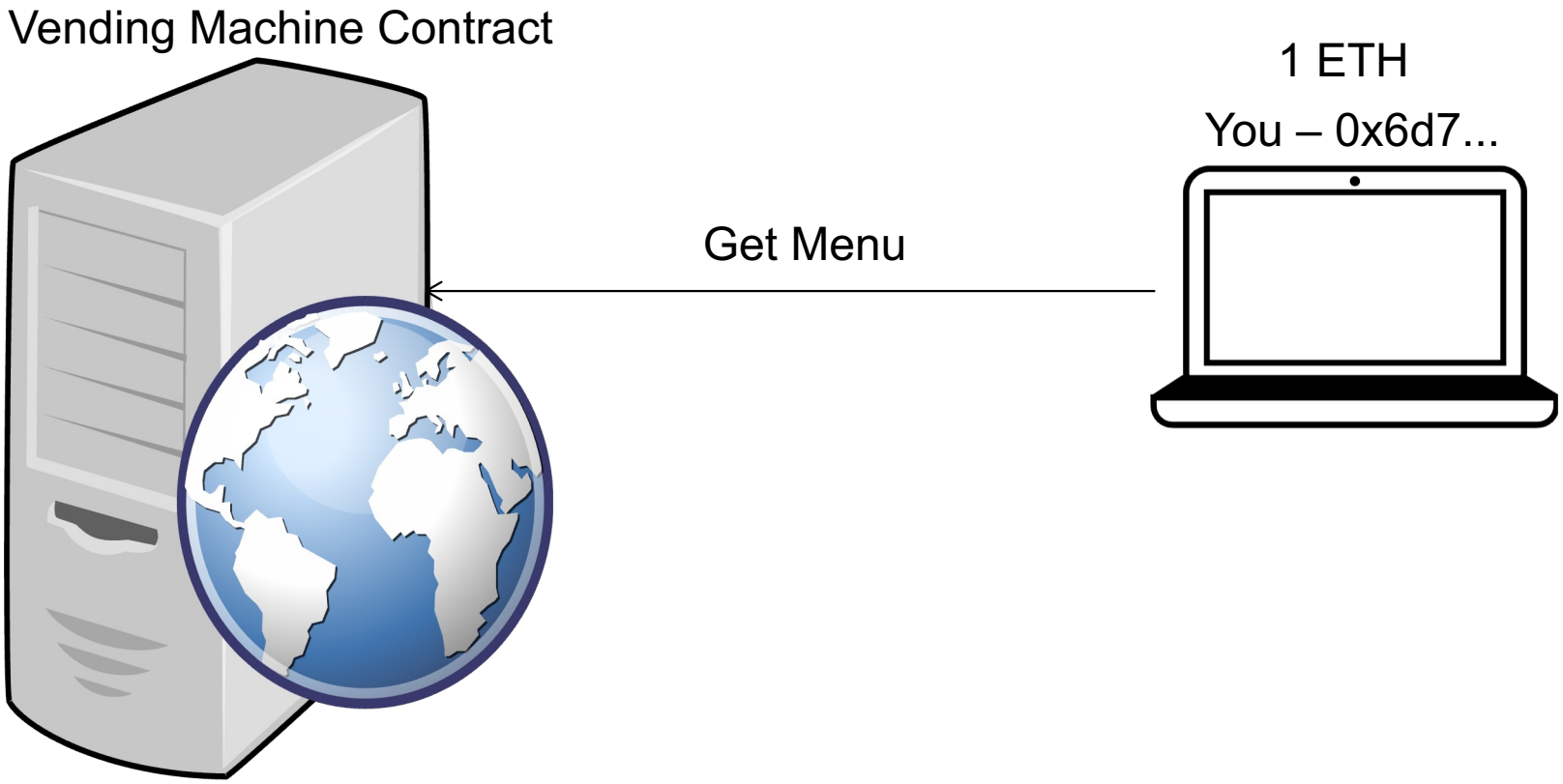
What is an ABI?

- Specifies how the contract is called
- Address is where the contract lives
- ABI is how to talk to the contract

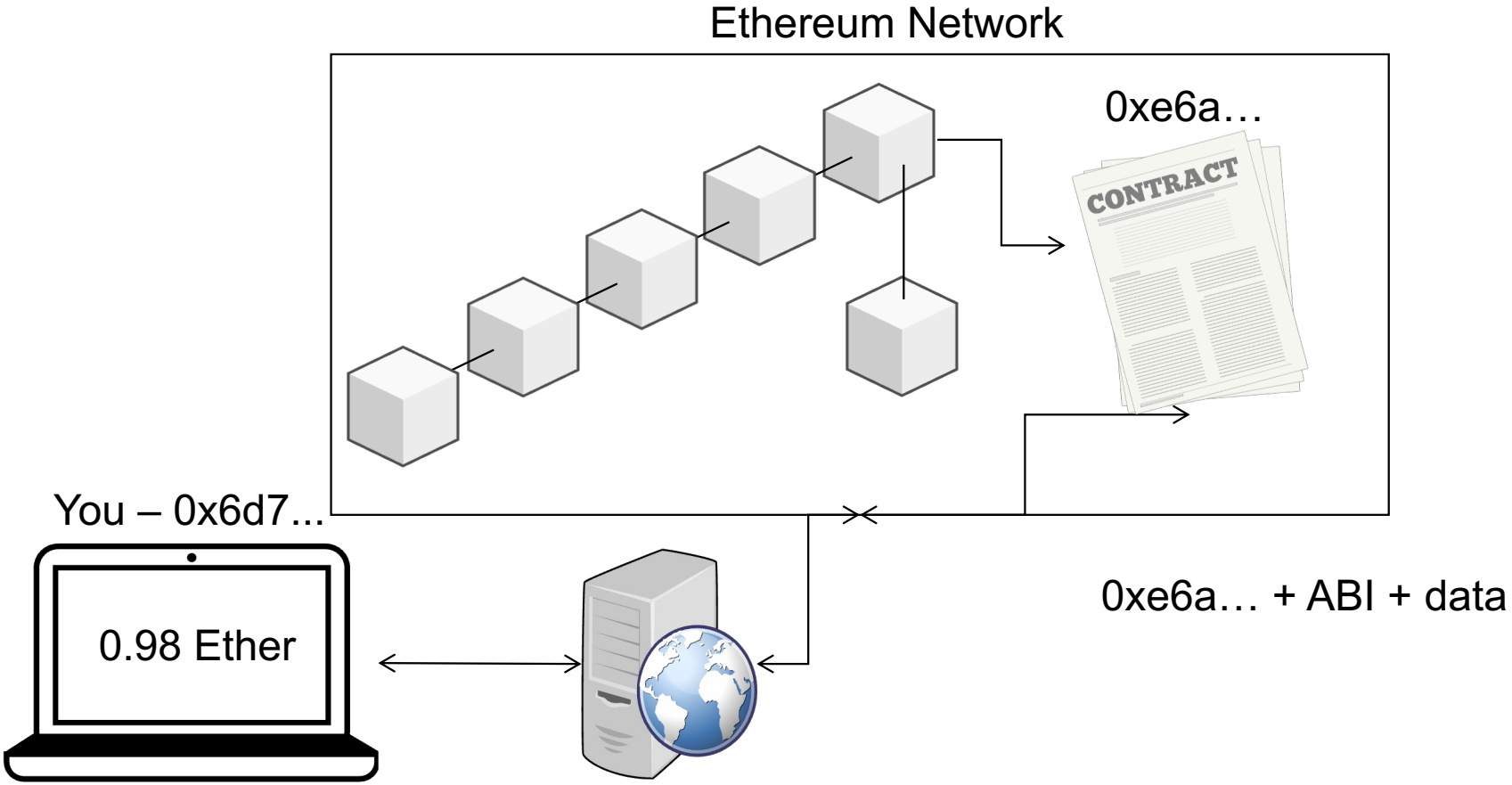
Sending a Transaction to a Smart Contract



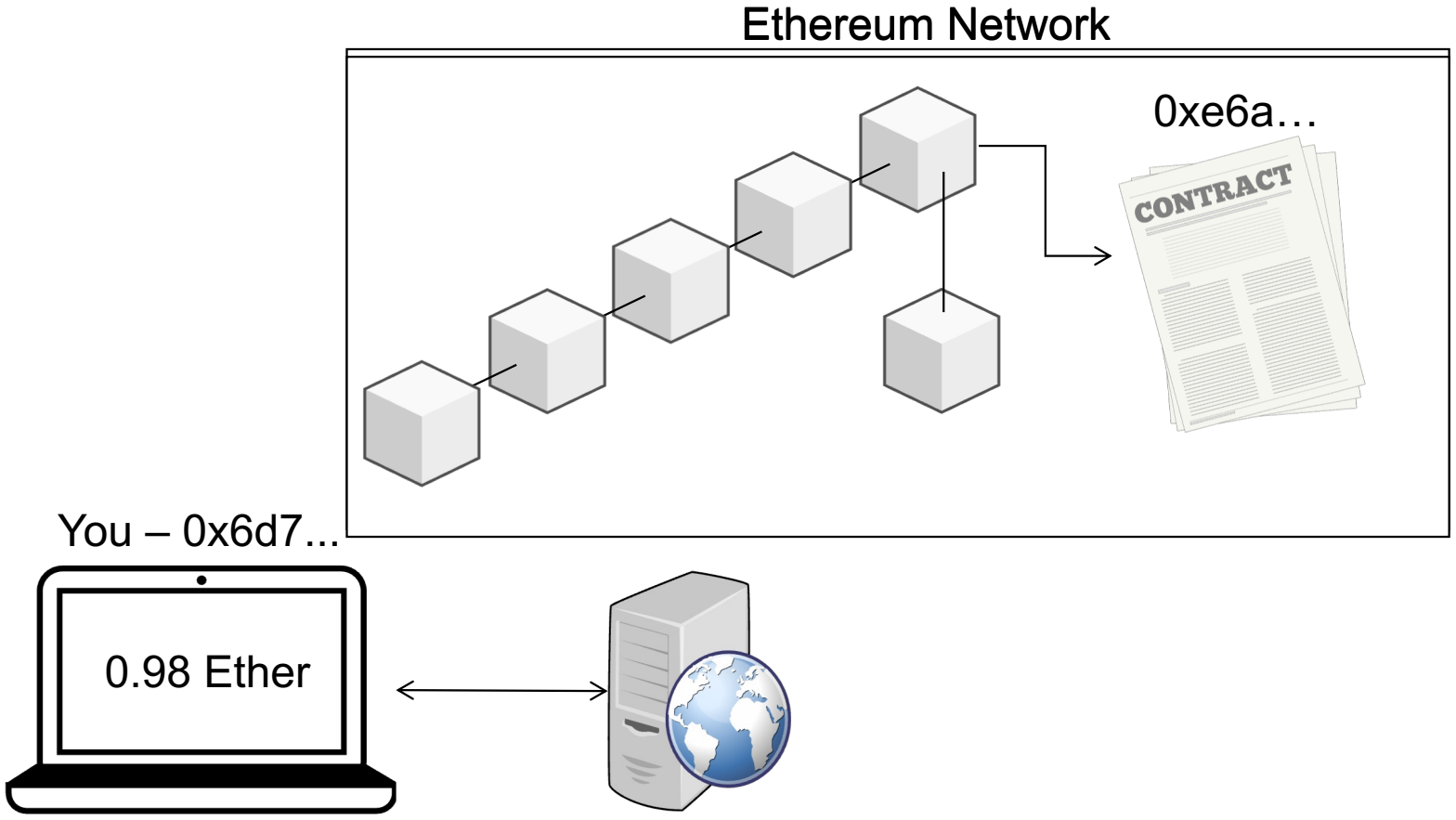
What does Outside of the Ethereum Network mean?



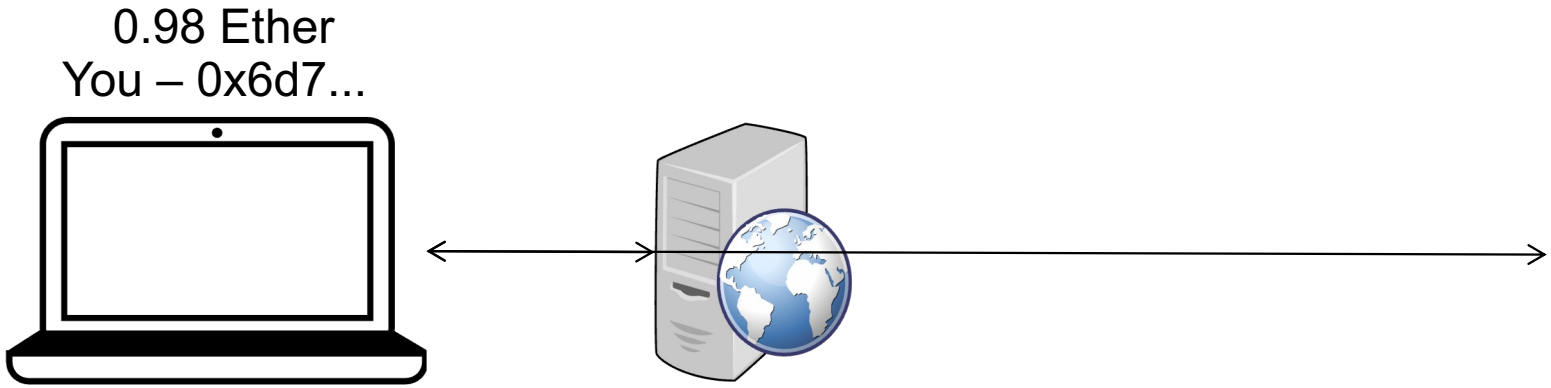
Calling a Smart Contract



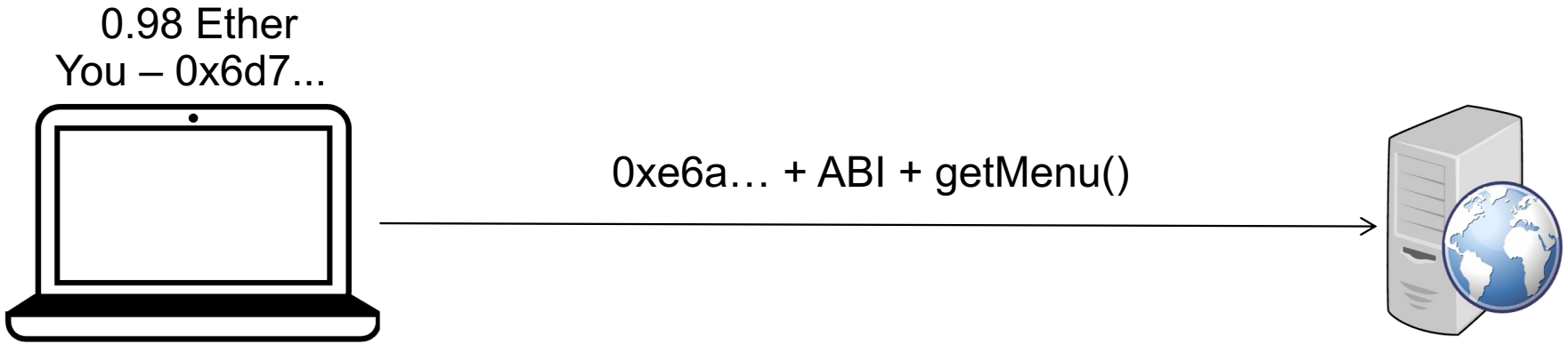
Calling a Smart Contract



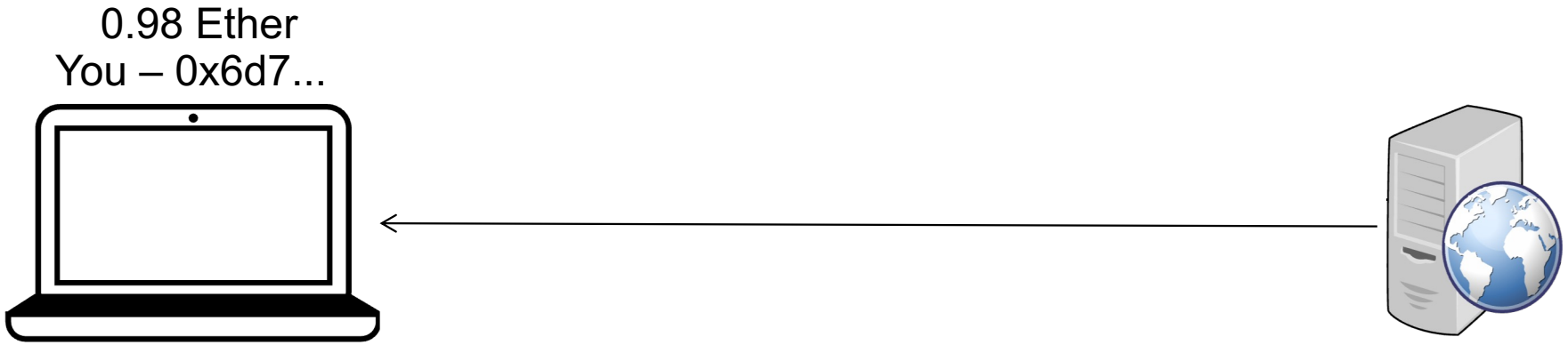
Calling a Smart Contract



Calling a Smart Contract



Calling a Smart Contract



Rule of GAS

If the Ethereum Network is doing the processing,
it **WILL** cost GAS

GAS costs

- Within the Ethereum network, it costs GAS to do **EVERYTHING**
  - Transaction → Set Value
  - Transaction → Add 1 + 1
- Outside of the Ethereum network, it costs NO GAS but you **CANNOT CHANGE STATE** on the network
  - Call → Get Value
  - Call → Add 1 + 1

GAS costs using Transactions

Inside of the Ethereum Network

Set value

Add 1 + 1

Outside of the Ethereum Network

Get value

Add 1 + 1

NO GAS costs using Calls

Inside of the Ethereum Network

Set value

Add 1 + 1

Outside of the Ethereum Network

Get value

Add 1 + 1

Types of different Accounts

- Externally Owned Account
- Contract Account

Similarities between EOA and Contract Accounts

- Has an Address
- Has an Account Nonce
- Has a Balance

Difference between the Accounts?

- **Externally Owned Account**
- Contract Account

Externally Owned Account

- Has no Ethereum Virtual Machine code associated with it

Difference between the Accounts?

- Externally Owned Account
- **Contract Account**

Contract Account

- Also called an Autonomous Object
- Has Ethereum Virtual Machine Code associated with it
- Can manipulate its storage

Cases to Call?

- Want to test out what the result would be
  - Dry run
- Want to get a value that is stored on the Blockchain

Cases to Send Transaction?

- Want to change state on the Blockchain
  - Sending another person Ether
  - Verifying documents
  - Storing data

GAS costs

G_{create}	32000	Paid for a CREATE operation.
$G_{codedeposit}$	200	Paid per byte for a CREATE operation to succeed in placing code into state.
G_{call}	700	Paid for a CALL operation.
$G_{callvalue}$	9000	Paid for a non-zero value transfer as part of the CALL operation.
$G_{callstipend}$	2300	A stipend for the called contract subtracted from $G_{callvalue}$ for a non-zero value tr
$G_{newaccount}$	25000	Paid for a CALL or SELFDESTRUCT operation which creates an account.
G_{exp}	10	Partial payment for an EXP operation.
$G_{expbyte}$	50	Partial payment when multiplied by $\lceil \log_{256}(exponent) \rceil$ for the EXP operation.
G_{memory}	3	Paid for every additional word when expanding memory.
G_{txcreate}	32000	Paid by all contract-creating transactions after the *Homestead* transition.
$G_{txdatazero}$	4	Paid for every zero byte of data or code for a transaction.
$G_{txdatanonzero}$	68	Paid for every non-zero byte of data or code for a transaction.
$G_{transaction}$	21000	Paid for every transaction.

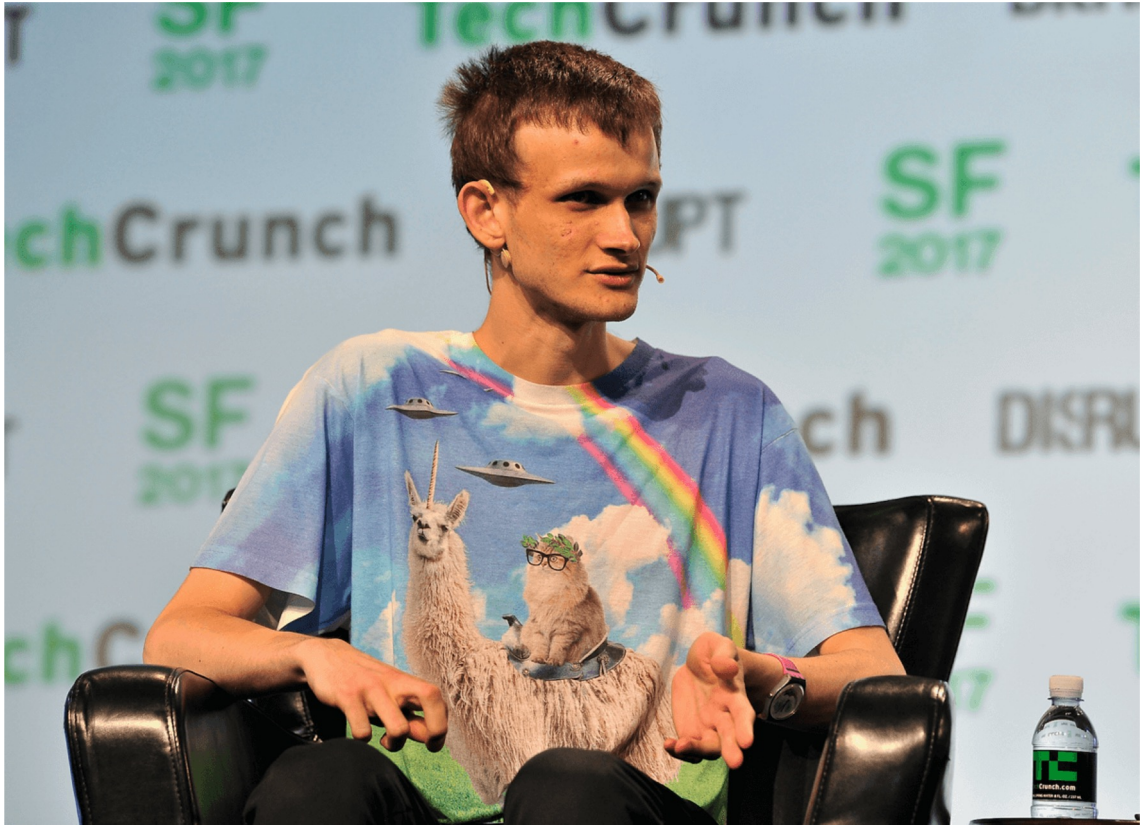
Why should I not store data?

- Storage is expensive
- Storage is VERY expensive
- A base Transaction costs 21,000 GAS
- Storing “Hello World!” costs 20,000 GAS
- Getting the “Hello World!”
  - Costs 800 GAS Internal (Transaction) to the EVM
  - Costs 0 GAS External (Call) to the EVM

How Expensive is Storage?

- Storing 256 bits of data costs 20,000 GAS
- 1 word = 256 bits
- 256 bits = 32 bytes = 1 word
- 32 bytes = 0.03125 kilobytes
- 0.03125 kilobytes = 0.00003125 megabytes

Example



= 358.3 kB
(358,297 b

How Expensive is Storage?

- 358,297 bytes / 32 = 11196.78125 = 11197 words
- 11197 words * 20,000 GAS + 21,000 GAS = 223940000 GAS
- 223,940,000 GAS * 100 Gwei = 22,394,000,000 Gwei
- 22,396,100,000 Gwei = 22.3961 ETH
- 22.3961 ETH = **35,898.48 CAD**
- Gas Limit of a Block is 10,000,000 GAS

Example

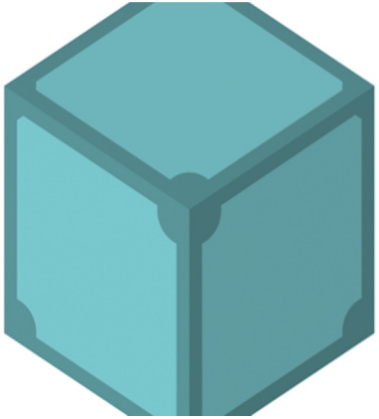
= 8.0 kB (7,9

How Expensive is Storage?

- 7,951 bytes / 32 = 248.46875 = 249 words
- 249 words * 20,000 GAS + 21,000 GAS = 5,001,000 GAS
- 5,001,000 GAS * 100 Gwei = 500,100,000 Gwei
- 500,100,000 Gwei = 0.5001 ETH
- 0.5001 ETH = **795.28 CAD**

Where can I store data?

- IPFS
- Swarm
- Database



IPFS

swarm

Where do Smart Contracts fit into a Decentralized Application?

Smart Contracts are the back end of a Decentralized Application

What we learned

- What a Smart Contract is
- The uses of a Smart Contract
- The difference between a Call and a Send Transaction
- The difference between a EOA and a Contract Account
- Why we should not store a large amount of data on the Blockchain
- Smart Contracts act as the back end of a Dapp

WHAT IS METIS?

FUTURE DECENTRALIZED ECONOMY PLATFORM FOR BUSINESS AND COMMUNITY

MISSION

To accelerate the transition of people to blockchain for open, fair, and decentralized business on Web 3.0.

VISION

To create an easy-to-use technical and organizational platform, making blockchain accessible to everyone and empowering both personal and professional lives.

METIS.IO

USE CASES

- DAO
- Launchpads
- DeFi
- Freelancing
- DApp
- Tokenization
- NFT
- Decentralized Exchanges

METIS.IO

Do these problems sound familiar?

METIS

SOLVED!

METIS.IO

HATE PAYING HIGH GAS FEES?

Only a few cents on Metis Layer 2

TIRED OF SLOW TRANSACTIONS?

Processed in a few seconds, with no bottlenecks

SUPER EXPENSIVE TO STORE DATA ON ETHEREUM?

Secure, cheap, permissioned off-chain storage, pre-built for your project needs

CODING SMART CONTRACTS FROM SCRATCH DOESN'T FEEL SO SMART?

One-click templates and deployments

CONCERNED WITH CENTRALIZED PRIVATE SIDECHAIN RISKS?

All decentralized. All on Ethereum. **Only with Metis!**

Subscribe to stay tuned at

METIS.IO

t.me/MetisDAO