Crypto for Dummies

Natasha Che, Alex Copestake

December 15, 2021

Disclaimers

- Not an expert

- Massive question, short time =
  - V simplified, v happy to discuss in more detail any time

References

- Blockchain 101 - A Visual Demo – YouTube
  - 17 min illustration of the technological building blocks
- Some simple economics of the blockchain | Communications of the ACM
  - 11 pages discussing potential economic impacts (Catalini & Gans)
- Blockchain: Foundations and Use Cases - Home | Coursera
  - Many lectures, from basics to technical details
- Video Lectures | Blockchain and Money | Sloan School of Management | MIT OpenCourseWare
  - Gary Gensler (now SEC Chair) course on potential impacts on finance

Plan

- A paper blockchain
- A Google Sheets blockchain

➔ **Bitcoin**

- Custom-column distributed spreadsheets with formulae

➔**Ethereum**

➔**DeFi, briefly**

- Chain of Title

➔ **NFTs**

Plan

- A paper blockchain
- A Google Sheets blockchain

➔ **Bitcoin is a spreadsheet**

- Custom-column distributed spreadsheets with formulae

➔**Ethereum**

➔**DeFi, briefly**

- Chain of Title

➔ **NFTs**

Plan

- A paper blockchain
- A Google Sheets blockchain

➔ **Bitcoin is a spreadsheet**

- Custom-column distributed spreadsheets with formulae

➔**Ethereum is a spreadsheet with formulae**

➔**DeFi, briefly**

- Chain of Title

➔ **NFTs**

Plan

- A paper blockchain
- A Google Sheets blockchain

➔ **Bitcoin is a spreadsheet**

- Custom-column distributed spreadsheets with formulae

➔ **Ethereum is a spreadsheet with formulae**

➔ **DeFi, briefly is spreadsheets talking to spreadsheets (=DMX??)**

- Chain of Title

➔ **NFTs**

Plan

- A paper blockchain
- A Google Sheets blockchain

➔ **Bitcoin is a spreadsheet**

- Custom-column distributed spreadsheets with formulae

➔ **Ethereum is a spreadsheet with formulae**

➔ **DeFi, briefly is spreadsheets talking to spreadsheets (=DMX??)**

- Chain of Title

➔ **NFTs are also spreadsheets**

Analogy #1: A paper blockchain

Block	Sender	Recipient	Amount	Time
1	.	Alice	10	01/01/0000 09:00:00

This is a piece of paper, showing that:

Analogy #1: A paper blockchain

Block	Sender	Recipient	Amount	Time
1	.	Alice	10	01/01/0000 09:00:00

This is a piece of paper, showing that:
Alice starts with 10 units

Analogy #1: A paper blockchain

Block	Sender	Recipient	Amount	Time
1	.	Alice	10	01/01/0000 09:00:00

Block	Sender	Recipient	Amount	Time
?	Alice	Bob	5	02/01/0000 09:00:00

This is another piece of paper, showing that:

Analogy #1: A paper blockchain

Block	Sender	Recipient	Amount	Time
1	.	Alice	10	01/01/0000 09:00:00

Block	Sender	Recipient	Amount	Time
?	Alice	Bob	5	02/01/0000 09:00:00

This is another piece of paper, showing that:
Alice wants to transfer 5 to Bob

Analogy #1: A paper blockchain

Block	Sender	Recipient	Amount	Time
1	.	Alice	10	01/01/0000 09:00:00

Block	Sender	Recipient	Amount	Time
?	Alice	Bob	5	02/01/0000 09:00:00

The Miner (more on them later) looks back at the previous transactions, to see whether Alice has enough units to pay 5 to Bob

Analogy #1: A paper blockchain

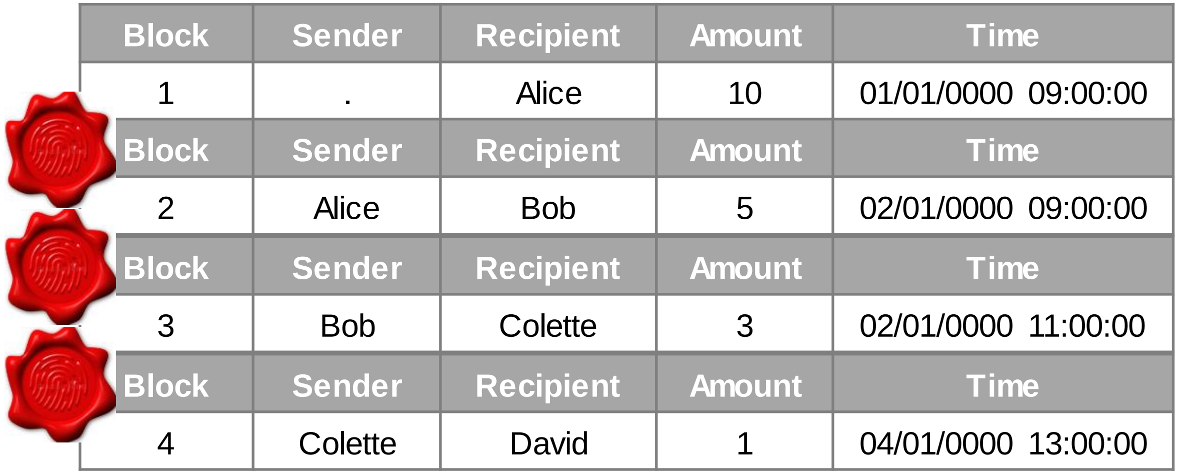
Block	Sender	Recipient	Amount	Time
1	.	Alice	10	01/01/0000 09:00:00

Block	Sender	Recipient	Amount	Time
2	Alice	Bob	5	02/01/0000 09:00:00

Alice does, so the transaction is added to the first, and sealed with the Miner's fingerprint in wax

(For simplicity, taking block size = 1 transaction)

Analogy #1: A paper blockchain



Block	Sender	Recipient	Amount	Time
1	.	Alice	10	01/01/0000 09:00:00

Block	Sender	Recipient	Amount	Time
2	Alice	Bob	5	02/01/0000 09:00:00

Block	Sender	Recipient	Amount	Time
3	Bob	Colette	3	02/01/0000 11:00:00

Block	Sender	Recipient	Amount	Time
4	Colette	David	1	04/01/0000 13:00:00

Repeating this over and over gives a long chain of valid and validated transactions, that anyone can go and look at

If someone tore one block out, it would be immediately obvious

Analogy #1: A paper blockchain

Block	Sender	Recipient	Amount	Time
1	.	Alice	10	01/01/0000 09:00:00

Block	Sender	Recipient	Amount	Time
2	Alice	Bob	5	02/01/0000 09:00:00

Block	Sender	Recipient	Amount	Time
3	Bob	Colette	3	02/01/0000 11:00:00

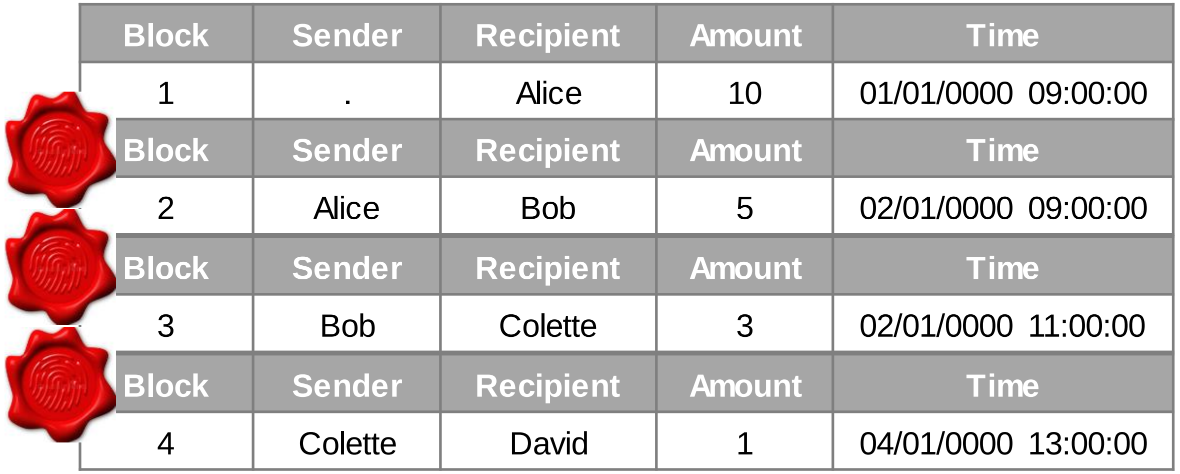
Block	Sender	Recipient	Amount	Time
4	Colette	David	1	04/01/0000 13:00:00

At any given moment, we could work out the distribution of assets by summing backwards across the chain:

Alice	=	10 - 5	= 5
Bob	=	5 - 3	= 2
Colette	=	3-1	= 2
David	=	1	

Total = 10

Analogy #1: A paper blockchain

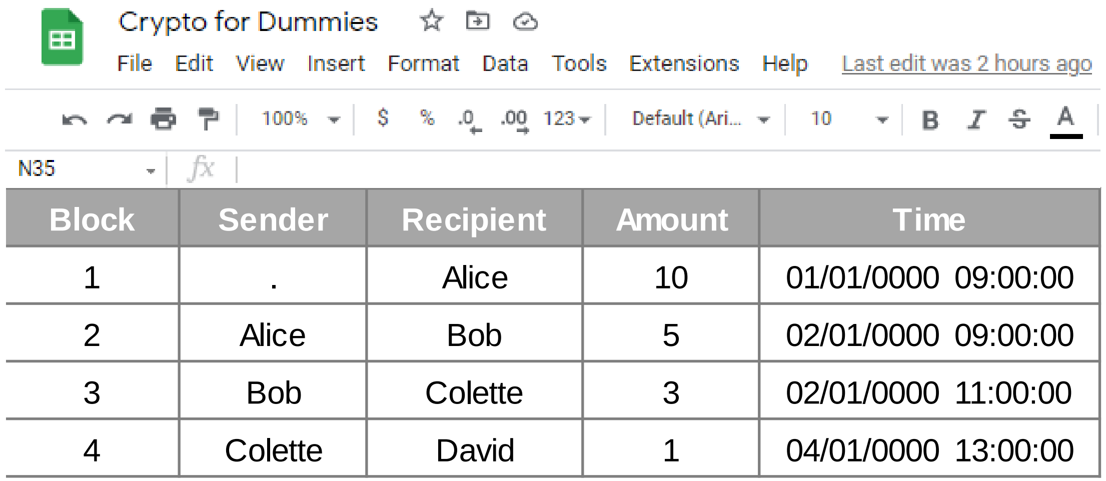


Block	Sender	Recipient	Amount	Time
1	.	Alice	10	01/01/0000 09:00:00
Block	Sender	Recipient	Amount	Time
2	Alice	Bob	5	02/01/0000 09:00:00
Block	Sender	Recipient	Amount	Time
3	Bob	Colette	3	02/01/0000 11:00:00
Block	Sender	Recipient	Amount	Time
4	Colette	David	1	04/01/0000 13:00:00

Assuming everyone has access to the long chain of paper, it’s visible to everyone…

But obviously, hard to scale up using paper…

Analogy #2: A Google Sheets blockchain

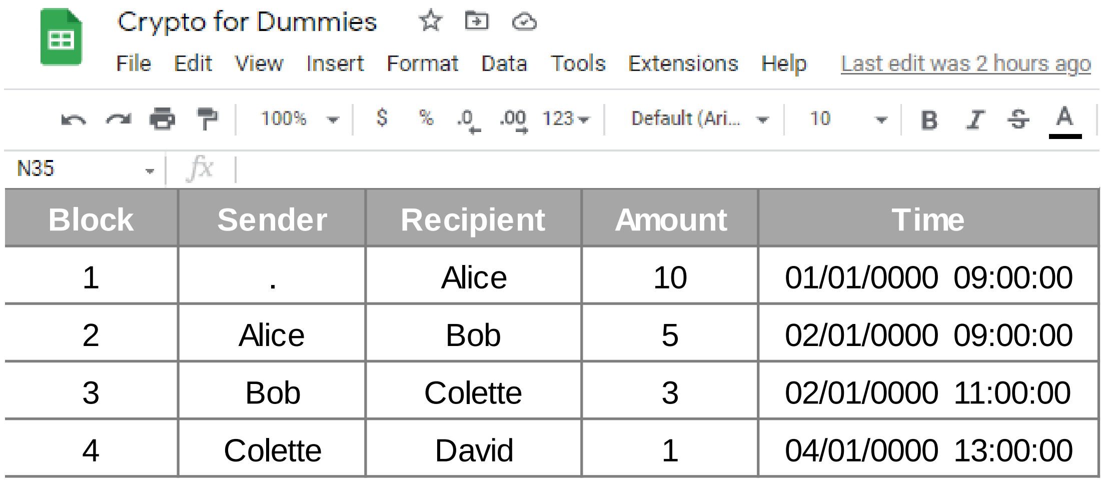

Crypto for Dummies
File Edit View Insert Format Data Tools Extensions Help
Last edit was 2 hours ago
100%
$ % .0 .00 123
Default (Ari...
10
B I S A
N35
fx

Block	Sender	Recipient	Amount	Time
1	.	Alice	10	01/01/0000 09:00:00
2	Alice	Bob	5	02/01/0000 09:00:00
3	Bob	Colette	3	02/01/0000 11:00:00
4	Colette	David	1	04/01/0000 13:00:00

Now everyone can see it simultaneously!

But: how to verify?

Analogy #2: A Google Sheets blockchain



Block	Sender	Recipient	Amount	Time
1	.	Alice	10	01/01/0000 09:00:00
2	Alice	Bob	5	02/01/0000 09:00:00
3	Bob	Colette	3	02/01/0000 11:00:00
4	Colette	David	1	04/01/0000 13:00:00

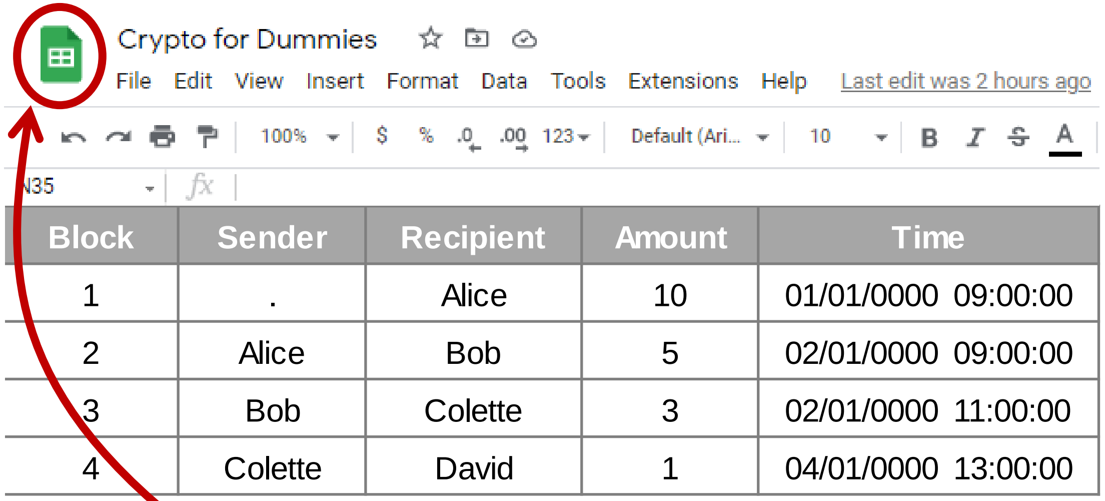
Now everyone can see it simultaneously!

But: how to verify?

One option:

1. Make the Sheet ‘View only’
2. Everyone sends their desired transactions to Google (creating a ‘mempool’ of candidate transactions)
3. Google checks if everyone has enough assets to make their desired transaction
4. If yes, accept it and add to chain

Analogy #2: A Google Sheets blockchain



Block	Sender	Recipient	Amount	Time
1	.	Alice	10	01/01/0000 09:00:00
2	Alice	Bob	5	02/01/0000 09:00:00
3	Bob	Colette	3	02/01/0000 11:00:00
4	Colette	David	1	04/01/0000 13:00:00

Problem: centralized!
Google can charge large
markup, sell our data etc.

Now everyone can see it simultaneously!

But: how to verify?

One option:

1. Make the Sheet 'View only'
2. Everyone sends their desired transactions to Google (creating a 'mempool' of candidate transactions)
3. Google checks if everyone has enough assets to make their desired transaction
4. If yes, accept it and add to chain

Example #1: Bitcoin

Block	Sender	Recipient	Amount	Time
1	.	Alice	10	01/01/0000 09:00:00
2	Alice	Bob	5	02/01/0000 09:00:00
3	Bob	Colette	3	02/01/0000 11:00:00
4	Colette	David	1	04/01/0000 13:00:00

Problem: centralized!
Google can charge large
markup, sell our data etc.

Solution:

1. List of past valid transactions is hosted simultaneously on many computers (‘distributed ledger’ across many ‘nodes’). As long as there’s no critical mass of malicious nodes, no-one can tamper with past transactions

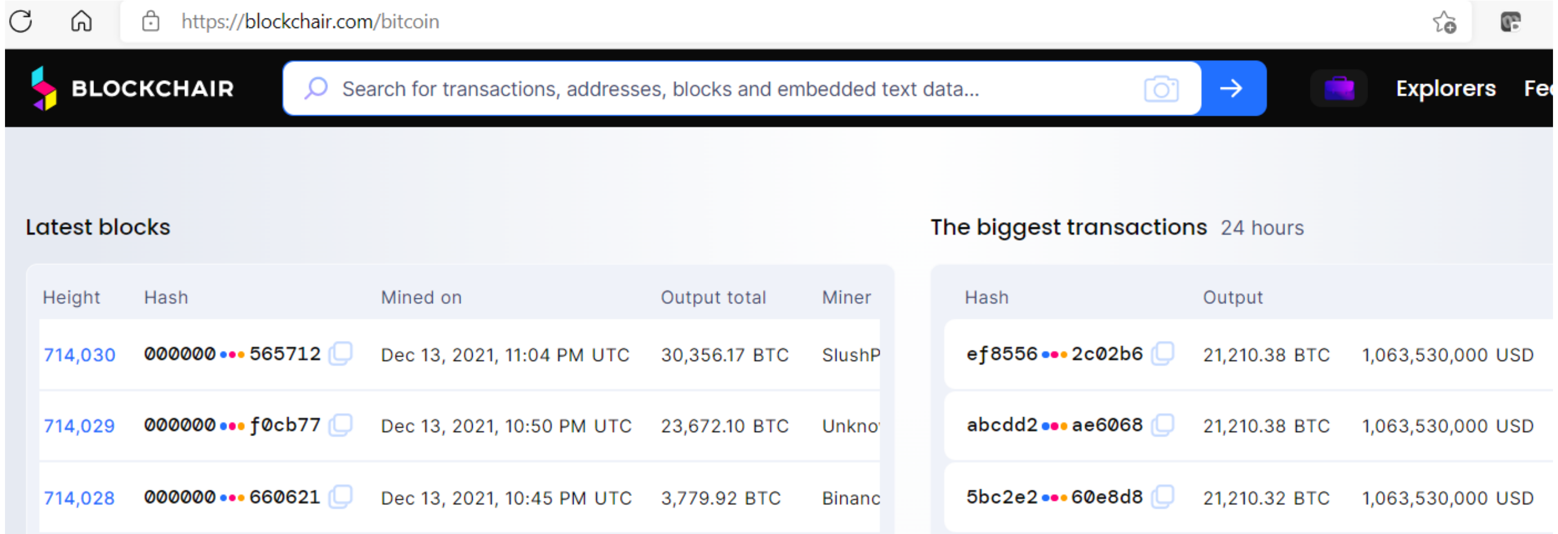
Example #1: Bitcoin

Block	Sender	Recipient	Amount	Time
1	*.*	*Alice*	*10*	*01/01/0000 09:00:00*
2	*Alice*	*Bob*	*5*	*02/01/0000 09:00:00*
3	*Bob*	*Colette*	*3*	*02/01/0000 11:00:00*

Past

Solution:

1. List of past valid transactions is hosted simultaneously on many computers ('distributed ledger' across many 'nodes'). As long as there's no critical mass of malicious nodes, no-one can tamper with past transactions



https://blockchair.com/bitcoin

BLOCKCHAIR

Search for transactions, addresses, blocks and embedded text data...

Explorers Fe

Latest blocks

Height	Hash	Mined on	Output total	Miner
714,030	000000 ••• 565712	Dec 13, 2021, 11:04 PM UTC	30,356.17 BTC	SlushP
714,029	000000 ••• f0cb77	Dec 13, 2021, 10:50 PM UTC	23,672.10 BTC	Unkno
714,028	000000 ••• 660621	Dec 13, 2021, 10:45 PM UTC	3,779.92 BTC	Binanc

The biggest transactions 24 hours

Hash	Output	
ef8556 ••• 2c02b6	21,210.38 BTC	1,063,530,000 USD
abcdd2 ••• ae6068	21,210.38 BTC	1,063,530,000 USD
5bc2e2 ••• 60e8d8	21,210.32 BTC	1,063,530,000 USD

Example #1: Bitcoin

Block	Sender	Recipient	Amount	Time
1	.	*Alice*	*10*	*01/01/0000 09:00:00*
2	*Alice*	*Bob*	*5*	*02/01/0000 09:00:00*
3	*Bob*	*Colette*	*3*	*02/01/0000 11:00:00*

Past

Block	Sender	Recipient	Amount	Time
4	Colette	David	1	04/01/0000 13:00:00

New

Solution:

1. List of past valid transactions is hosted simultaneously on many computers (‘distributed ledger’ across many ‘nodes’). As long as there’s no critical mass of malicious nodes, no-one can tamper with past transactions
2. When users want to make a transaction, they again send it out into the ‘mempool’ of candidate transactions (as in the Google Sheets version)

Example #1: Bitcoin

Block	Sender	Recipient	Amount	Time
1	*.*	*Alice*	*10*	*01/01/0000 09:00:00*
2	*Alice*	*Bob*	*5*	*02/01/0000 09:00:00*
3	*Bob*	*Colette*	*3*	*02/01/0000 11:00:00*
4	Colette	David	1	04/01/0000 13:00:00

Past

New

Solution:

1. List of past valid transactions is hosted simultaneously on many computers (‘distributed ledger’ across many ‘nodes’). As long as there’s no critical mass of malicious nodes, no-one can tamper with past transactions
2. When users want to make a transaction, they again send it out into the ‘mempool’ of candidate transactions (as in the Google Sheets version)
3. But now many different Miners compete* to be the one that validates it, and adds it to the chain with their stamp…

Example #1: Bitcoin

Block	Sender	Recipient	Amount	Time
1	*.*	*Alice*	*10*	*01/01/0000 09:00:00*
2	*Alice*	*Bob*	*5*	*02/01/0000 09:00:00*
3	*Bob*	*Colette*	*3*	*02/01/0000 11:00:00*
4	Colette	David	1	04/01/0000 13:00:00

Past

New

Solution:

1. List of past valid transactions is hosted simultaneously on many computers (‘distributed ledger’ across many ‘nodes’). As long as there’s no critical mass of malicious nodes, no-one can tamper with past transactions
2. When users want to make a transaction, they again send it out into the ‘mempool’ of candidate transactions (as in the Google Sheets version)
3. But now many different Miners compete* to be the one that validates it, and adds it to the chain with their stamp…
4. …For which they earn a reward in terms of new currency, which explains how new blockchain come into circulation.

Example #1: Bitcoin

Block	Sender	Recipient	Amount	Time
1	*.*	*Alice*	*10*	*01/01/0000 09:00:00*
2	*Alice*	*Bob*	*5*	*02/01/0000 09:00:00*
3	*Bob*	*Colette*	*3*	*02/01/0000 11:00:00*
4	Colette	David	1	04/01/0000 13:00:00

Past

New

*Usually through either:

- **Proof of Work** – solving a computationally intensive puzzle, the solution of which is nonetheless computationally easy for other nodes to verify;
- **Proof of Stake** – selecting validators in proportion to their existing holdings of the asset. Much cheaper + greener!

The key idea: these make it **costly to maliciously validate false transactions.** Bitcoin is PoW; Ethereum transitioning to PoS.

Solution:

1. List of past valid transactions is hosted simultaneously on many computers (‘distributed ledger’ across many ‘nodes’). As long as there’s no critical mass of malicious nodes, no-one can tamper with past transactions
2. When users want to make a transaction, they again send it out into the ‘mempool’ of candidate transactions (as in the Google Sheets version)
3. But now many different Miners compete* to be the one that validates it, and adds it to the chain with their stamp…
4. …For which they earn a reward in terms of new currency, which explains how new blockchain come into circulation.

Analogy #3: **Custom-column** distributed spreadsheets **with functions + macros**

So far so good… but couldn’t we do something more exciting with our distributed spreadsheet?

Block	Sender	Recipient	Amount	Time
1	*.*	*Alice*	*10*	*01/01/0000 09:00:00*
2	*Alice*	*Bob*	*5*	*02/01/0000 09:00:00*
3	*Bob*	*Colette*	*3*	*02/01/0000 11:00:00*
4	Colette	David	1	04/01/0000 13:00:00

Analogy #3: **Custom-column** distributed spreadsheets **with functions + macros**

So far so good… but couldn't we do something more exciting with our distributed spreadsheet?

Block	Variable 1	Variable 2	Variable 3	Variable 4	Variable 5	Variable 6	Variable 7	Variable 8	…
1									
2									
3									
4									

Analogy #3: **Custom-column** distributed spreadsheets **with functions + macros**

So far so good… but couldn't we do something more exciting with our distributed spreadsheet?

Block	Variable 1	Variable 2	Variable 3	Variable 4	Variable 5	Variable 6	Variable 7	Variable 8	…
1									
2									
3									
4									

'**Smart contract**' = a dumb program

Example #2: Ethereum

Block	Variable 1	Variable 2	Variable 3	Variable 4	Variable 5	Variable 6	Variable 7	Variable 8	…
1									
2									
3									
4									

Example #2: Ethereum

Block	Variable 1	Variable 2	Variable 3	Variable 4	Variable 5	Variable 6	Variable 7	Variable 8	…
1									
2									
3									
4									

We know we can record a digital currency in this format:

Variable 1 = “Sender”
Variable 2 = “Recipient”
Variable 3 = “Amount”
Variable 4 = “Time”

What else can we do?

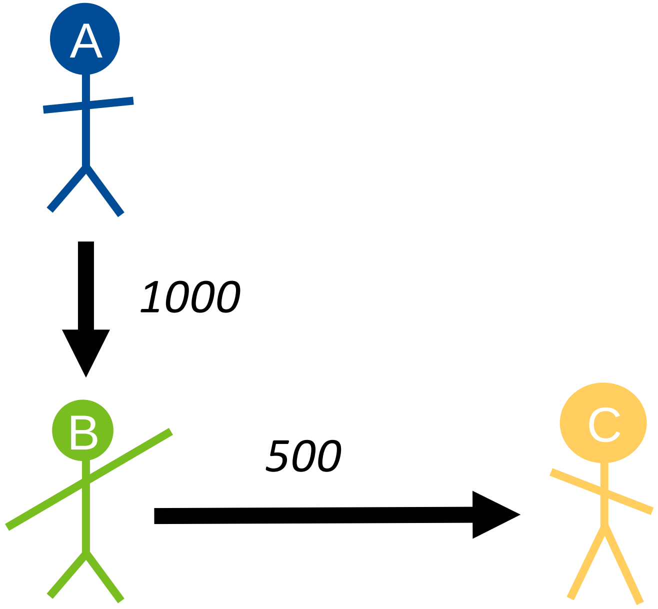
Example #2a: Ethereum rent-splitting smart contract

You and a friend co-own a property. Your tenant wants to pay you each in proportion to your ownership.

Example #2a: Ethereum rent-splitting smart contract

You and a friend co-own a property. Your tenant wants to pay you each in proportion to your ownership.

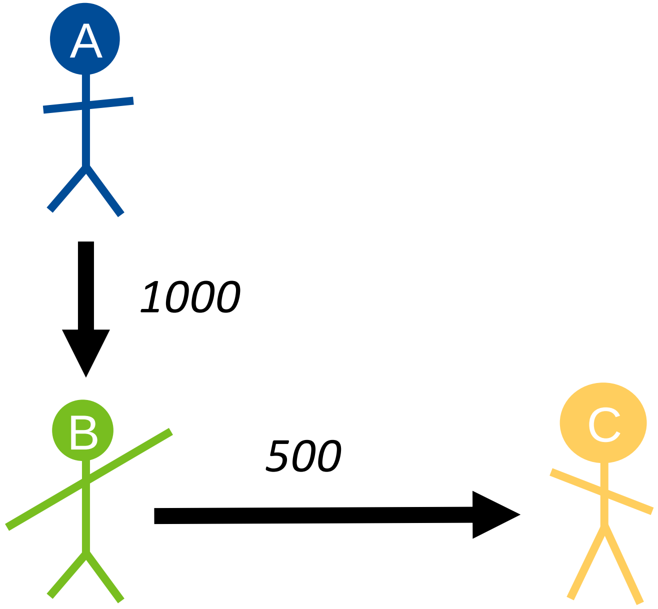
Without blockchain



Example #2a: Ethereum rent-splitting smart contract

You and a friend co-own a property. Your tenant wants to pay you each in proportion to your ownership.

Without blockchain

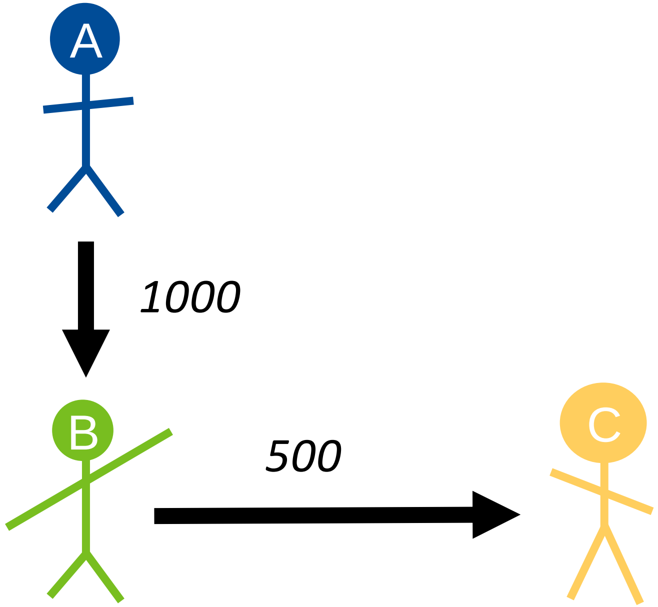


But what if B doesn't pass the money on to C?

Example #2a: Ethereum rent-splitting smart contract

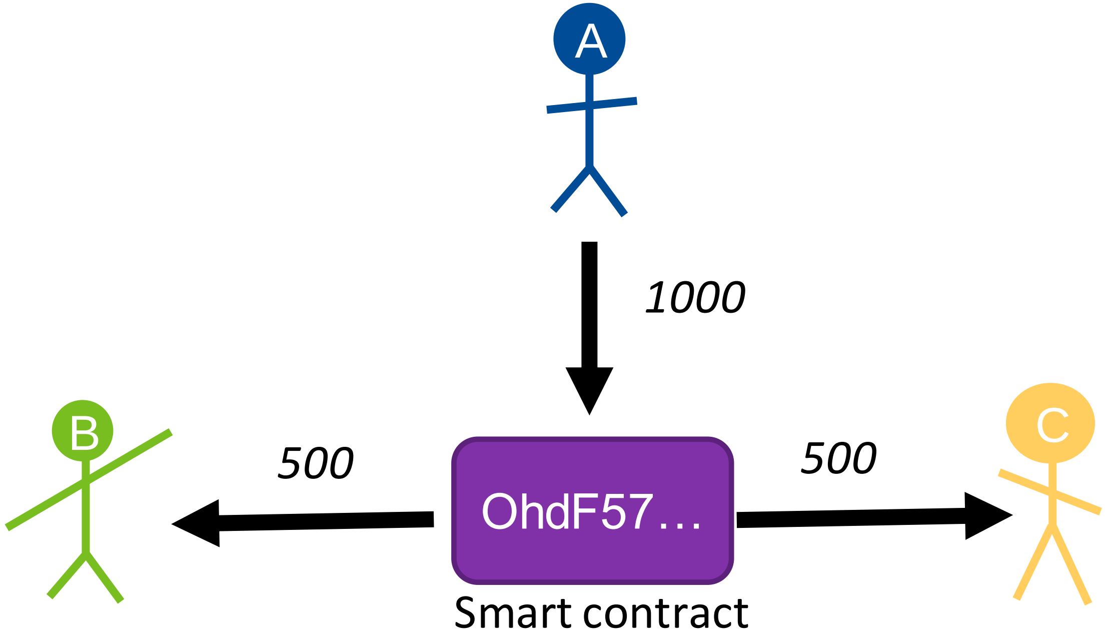
You and a friend co-own a property. Your tenant wants to pay you each in proportion to your ownership.

Without blockchain



But what if B doesn't pass the money on to C?

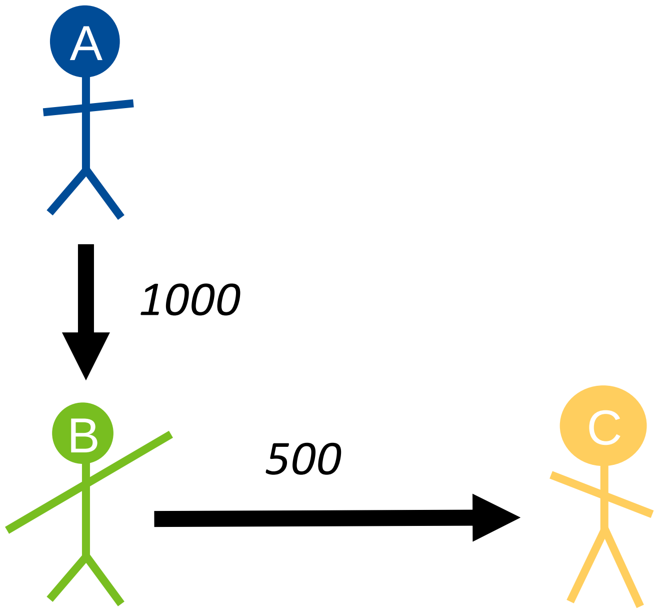
With smart contract on blockchain



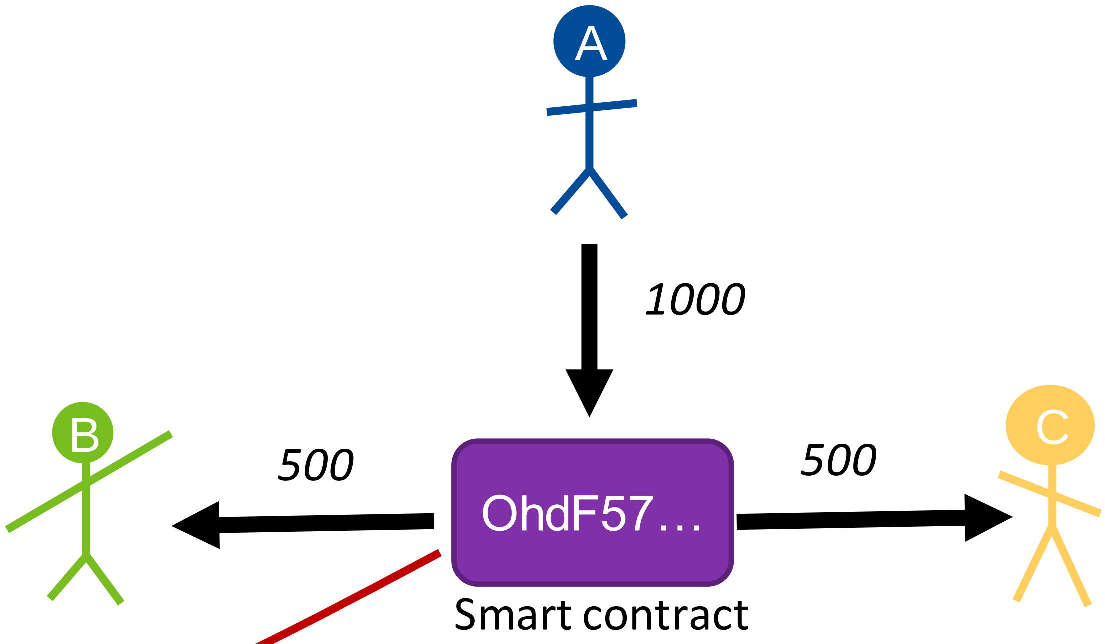
Example #2a: Ethereum rent-splitting smart contract

You and a friend co-own a property. Your tenant wants to pay you each in proportion to your ownership.

Without blockchain



With smart contract on blockchain



Smart contract

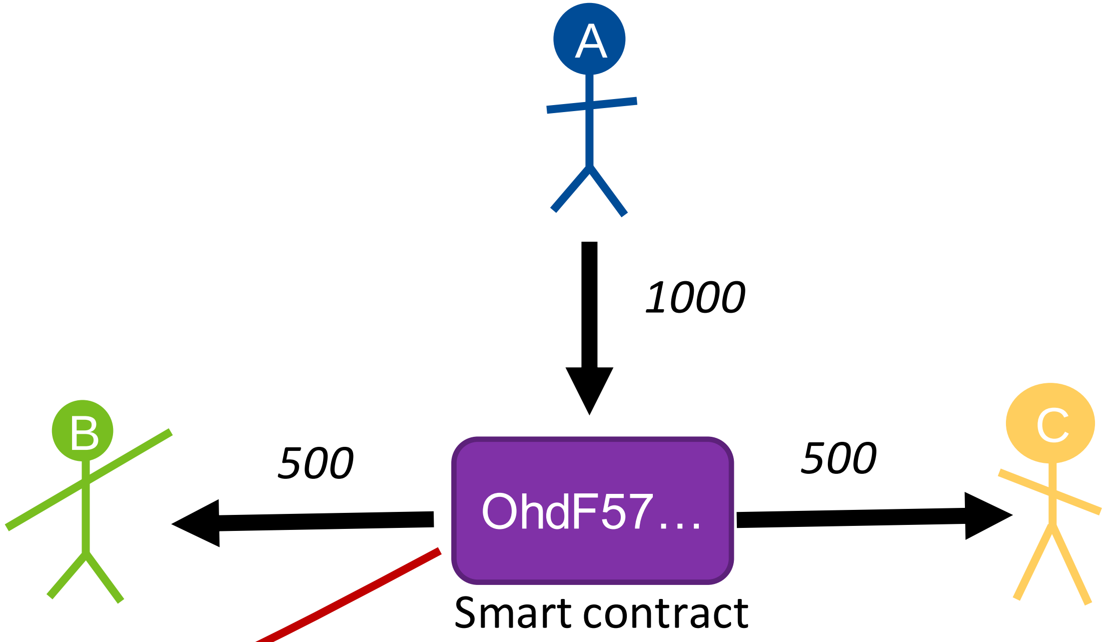
Block	Sender	Initial Recipient	Amount	Time	Owner 1	Owner 2	Owner 1 Share	Owner 2 Share	Owner 1 Amount	Owner 2 Amount
…										
5	A	OhdF57	1000	04/01/0000 13:00:00	B	C	50%	50%	= Share_1*Amount = 500	= Share_2*Amount = 500

Example #2a: Ethereum rent-splitting smart contract

You and a friend co-own a property. Your tenant wants to pay you each in proportion to your ownership.

With smart contract on blockchain

Why does this make things better?



Block	Sender	Initial Recipient	Amount	Time	Owner 1	Owner 2	Owner 1 Share	Owner 2 Share	Owner 1 Amount	Owner 2 Amount
…										
5	A	OhdF57	1000	04/01/0000 13:00:00	B	C	50%	50%	= Share_1*Amount = 500	= Share_2*Amount = 500

Example #2a: Ethereum rent-splitting smart contract

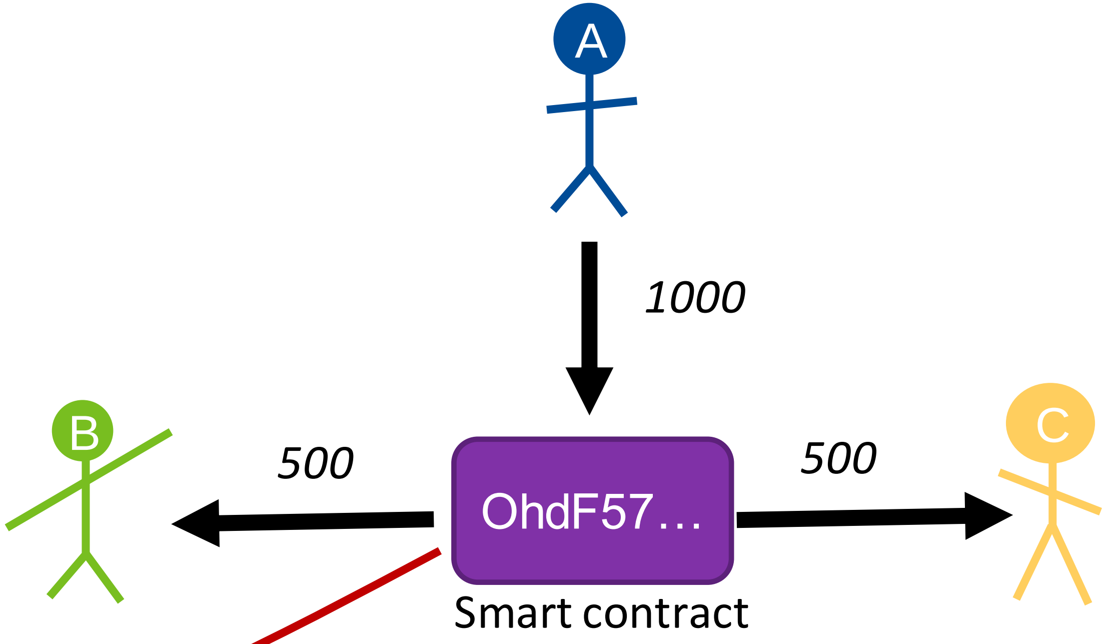
You and a friend co-own a property. Your tenant wants to pay you each in proportion to your ownership.

With smart contract on blockchain

Why does this make things better?

The smart contract is just code that anyone can verify, but no-one can tamper with without permission

- No trust required
- No expensive intermediary

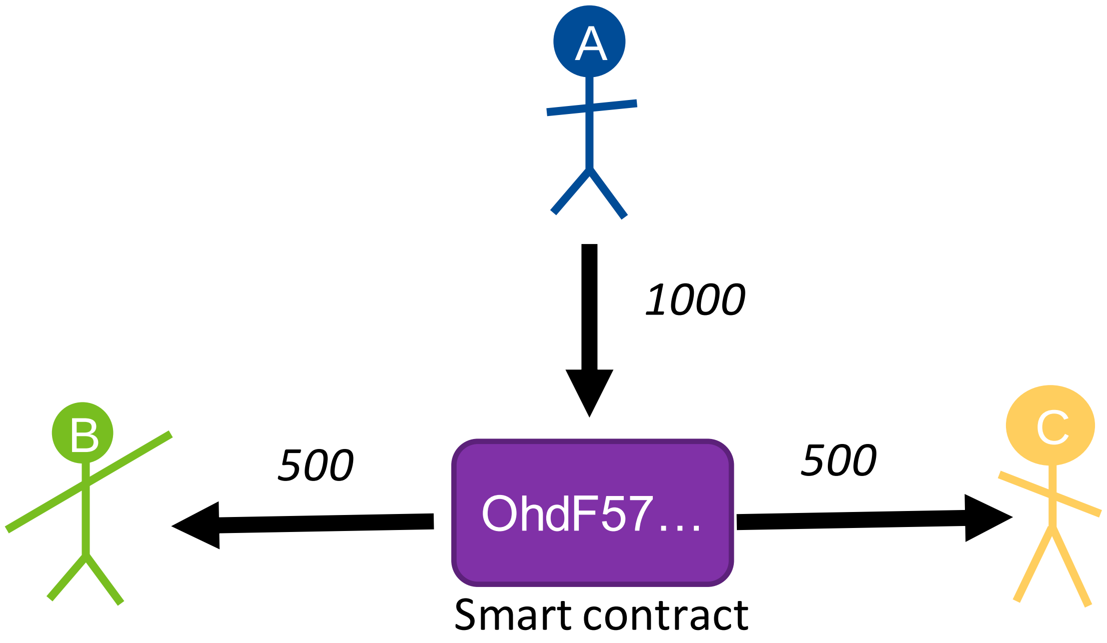


Block	Sender	Initial Recipient	Amount	Time	Owner 1	Owner 2	Owner 1 Share	Owner 2 Share	Owner 1 Amount	Owner 2 Amount
…										
5	A	OhdF57	1000	04/01/0000 13:00:00	B	C	50%	50%	= Share$_1$*Amount = 500	= Share$_2$*Amount = 500

Example #2a: Ethereum rent-splitting smart contract

You and a friend co-own a property. Your tenant wants to pay you each in proportion to your ownership.

With smart contract on blockchain



Why does this make things better?

The smart contract is just code that anyone can verify, but no-one can tamper with without permission

- No trust required
- No expensive intermediary

⇒ Becomes economical to have many more owners of property, being paid smaller shares = fractional ownership of property

Block	Sender	Initial Recipient	Amount	Time	Owner 1	Owner 2	Owner …	Owner 1 Share	Owner 2 Share	Owner … Share	Owner 1 Amount	Owner 2 Amount	Owner … Amount
…													
5	A	OhdF57	1000	04/01/0000 13:00:00	B	C		50%	50%		= S_1*Amount = 500	= S_2*Amount = 500	

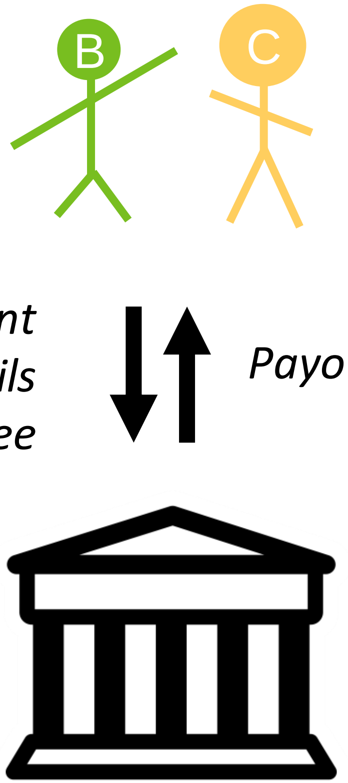
Example #2b: Ethereum derivatives

You bet your friend 0.5ETH that 1ETH will be worth >$5000 on January 1st 2023.

Example #2b: Ethereum derivatives

You bet your friend 0.5ETH that 1ETH will be worth >$5000 on January 1st 2023.

Without blockchain



Agreement
Account details
Transaction fee

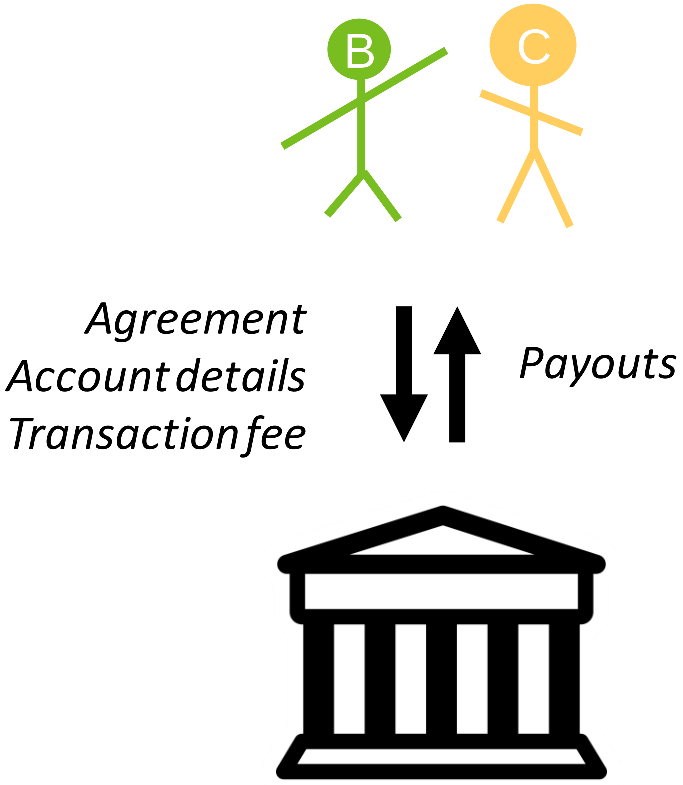
Payouts

Must be trusted

Example #2b: Ethereum derivatives

You bet your friend 0.5ETH that 1ETH will be worth >$5000 on January 1st 2023.

Without blockchain

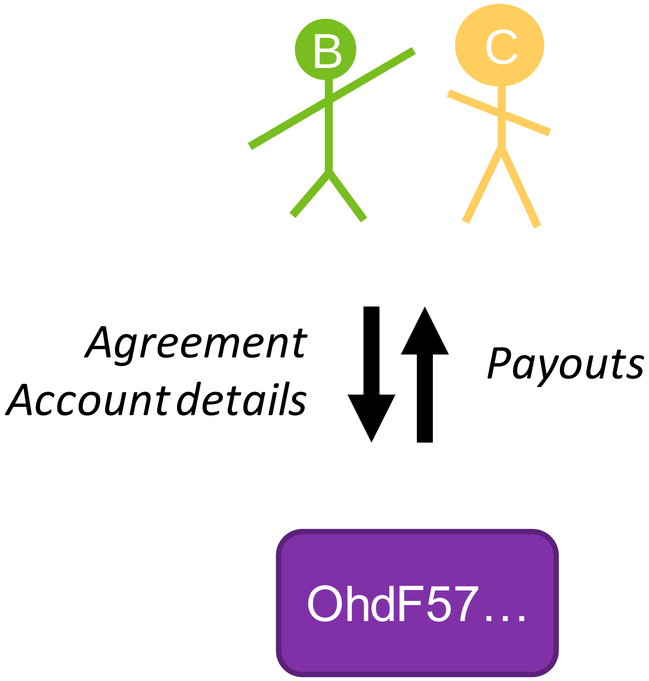


Agreement
Account details
Transaction fee

Payouts

Must be trusted

With smart contract on blockchain



Agreement
Account details

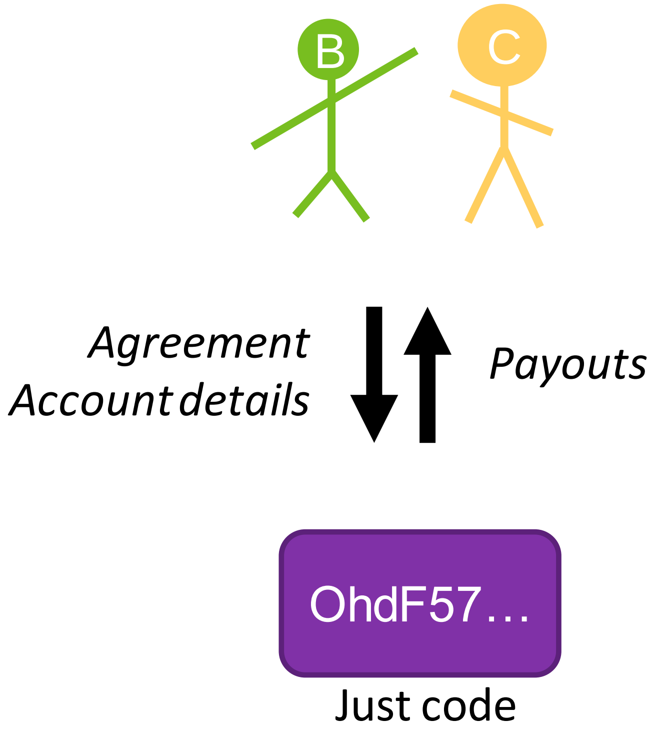
Payouts

Just code

Example #2b: Ethereum derivatives

You bet your friend 0.5ETH that 1ETH will be worth >$5000 on January 1st 2023.

With smart contract on blockchain

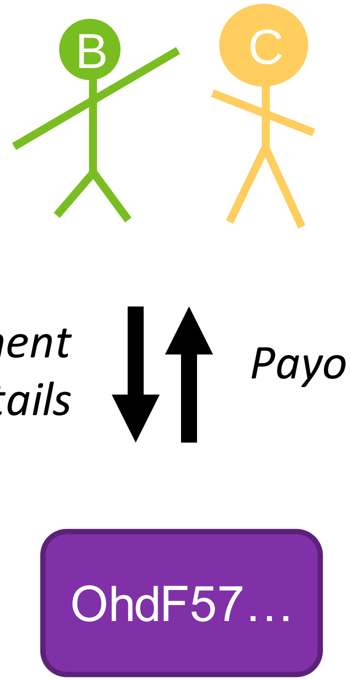


Block	Party 1	Party 2	Time	Validation Time	Value of 1 ETH	Bet Threshold	Bet Amount	Transaction
…								
5	B	C	04/01/0000 13:00:00	01/01/2023 00:00:00	?	$5000	0.5 ETH	= IF(“Time = Validation Time” & “Value of 1 ETH > Bet Threshold”, 0.5, -0.5)

Example #2b: Ethereum derivatives

You bet your friend 0.5ETH that 1ETH will be worth >$5000 on January 1st 2023.

With smart contract on blockchain



Agreement
Account details

Payouts

Just code

Provided by an ‘oracle’ = centralized or decentralized code linking to outside world. E.g. looks up price ETH:USD on website of currency exchange.

Work in progress! Last mile problems.

Block	Party 1	Party 2	Time	Validation Time	Value of 1 ETH	Bet Threshold	Bet Amount	Transaction
…								
5	B	C	04/01/0000 13:00:00	01/01/2023 00:00:00	?	$5000	0.5 ETH	= IF(“Time = Validation Time” & “Value of 1 ETH > Bet Threshold”, 0.5, -0.5)

Extension: Decentralized Finance (DeFi)

Example 2a

Block	Sender	Initial Recipient	Amount	Time	Owner 1	Owner 2	Owner 1 Share	Owner 2 Share	Owner 1 Amount	Owner 2 Amount
…										
5	A	OhdF57	1000	04/01/0000 13:00:00	B	C	50%	50%	= Share$_1$*Amount = 500	= Share$_2$*Amount = 500

Example 2b

Block	Party 1	Party 2	Time	Validation Time	Value of 1 ETH	Bet Threshold	Bet Amount	Transaction
…								
5	B	C	04/01/0000 13:00:00	01/01/2023 00:00:00	<from oracle>	$5000	0.5 ETH	= IF("Time = Validation Time" & "Value of 1 ETH > Bet Threshold", 0.5, -0.5)

Extensions to more complex forms of financial services straightforward

- Use more complex functions
- Combine multiple different blockchains, where the output of one is an input to another
- Use smart contracts running on one blockchain as building blocks for other smart contracts ➔ complex decentralized applications ('dapps')

E.g.

- Decentralized rent insurance that pays out if Example 2a rent never arrives
- Hedging products that combine many of the bets in Example 2b
- Decentralized exchange that will swap any cryptocurrency into any other at market rates
- Etc.

Analogy #4: Chain of Title

Before buying a flat, you check the chain of ownership to ensure the seller has the right to sell

Familiar?

Analogy #4: Chain of Title

Before buying a flat, you check the chain of ownership to ensure the seller has the right to sell

Familiar?

Asset	Sender	Recipient	Amount	Time
The Flat	.	*Alice*	*1*	*01/01/0000 09:00:00*
Dollars	*Alice*	.	*0*	*"*
The Flat	*Alice*	*Bob*	*1*	*02/01/0000 09:00:00*
Dollars	*Bob*	*Alice*	*100*	*"*
The Flat	*Bob*	*Colette*	*1*	*02/01/0000 11:00:00*
Dollars	*Colette*	*Bob*	*200*	*"*

Each exchange of the flat is accompanied by a corresponding dollar payment

Analogy #4: Chain of Title

Before buying a flat, you check the chain of ownership to ensure the seller has the right to sell

Familiar?

Asset	Sender	Recipient	Amount	Time
The Flat	.	*Alice*	*1*	*01/01/0000 09:00:00*
Dollars	*Alice*	.	*0*	”
The Flat	*Alice*	*Bob*	*1*	*02/01/0000 09:00:00*
Dollars	*Bob*	*Alice*	*100*	”
The Flat	*Bob*	*Colette*	*1*	*02/01/0000 11:00:00*
Dollars	*Colette*	*Bob*	*200*	”

Each exchange of the flat is accompanied by a corresponding dollar payment

The extent to which this chain means Colette really ‘owns’ the house is a matter of social conventions

1. *Government/courts will recognize it*
2. *Police obey the courts*
3. *Police will enforce the right, if necessary.*

The chain of ownership is not the house. But it is considered to have value!

Example #3: Non-Fungible Tokens

Similarly, this picture is just pixels.

Example #3: Non-Fungible Tokens

Similarly, this picture is just pixels.

But if I am considered its legitimate originator, and I publicly record that I have 'transferred it' to someone else, then they are now the legitimate owner.

We can record the resulting chain of transactions in another ~~public distributed spreadsheet~~ blockchain

Example #3: Non-Fungible Tokens

Similarly, this picture is just pixels.

But if I am considered its legitimate originator, and I publicly record that I have 'transferred it' to someone else, then they are now the legitimate owner.

We can record the resulting chain of transactions in another ~~public distributed spreadsheet~~ blockchain

Block	Asset	Sender	Recipient	Amount	Time
1	The Picture	.	*Alex*	*1*	*01/01/0000 09:00:00*
1	*ETH*	*Alex*	.	*0*	”
2	The Picture	*Alex*	*Bob*	*1*	*02/01/0000 09:00:00*
2	*ETH*	*Bob*	*Alex*	*100*	”
3	The Picture	*Bob*	*Colette*	*1*	*02/01/0000 11:00:00*
3	*ETH*	*Colette*	*Bob*	*200*	”

Again, for each candidate transaction, the Miner looks back up the chain to see if the Sender had the asset in their possession, such that they can legitimately sell it

Example #3: Non-Fungible Tokens

Similarly, this picture is just pixels.

But if I am considered its legitimate originator, and I publicly record that I have 'transferred it' to someone else, then they are now the legitimate owner.

We can record the resulting chain of transactions in another ~~public distributed spreadsheet~~ blockchain

Block	Asset	Sender	Recipient	Amount	Time
1	The Picture	*.*	*Alex*	*1*	*01/01/0000 09:00:00*
1	*ETH*	*Alex*	*.*	*0*	*”*
2	The Picture	*Alex*	*Bob*	*1*	*02/01/0000 09:00:00*
2	*ETH*	*Bob*	*Alex*	*100*	*”*
3	The Picture	*Bob*	*Colette*	*1*	*02/01/0000 11:00:00*
3	*ETH*	*Colette*	*Bob*	*200*	*”*

Again, for each candidate transaction, the Miner looks back up the chain to see if the Sender had the asset in their possession, such that they can legitimately sell it

Now, the extent to which this 'publicly verifiable claim to be the legitimate owner of the asset' actually has value is debatable – but people seem to think so at the moment (see graphs to follow ➔)

Example #3: Non-Fungible Tokens

So what actually is an NFT?

***Token** = a representation of something (e.g. movie ticket = right to legitimate entry to screening)*

***Non-fungible** = cannot be interchanged for other similar objects*

- *Unlike dollars, soybeans or gold*
- *The Mona Lisa, not just any picture or it*
- *My car, not just any version of the same model*

Block	Asset	Sender	Recipient	Amount	Time
1	The Picture	.	*Alex*	*1*	*01/01/0000 09:00:00*
1	*ETH*	*Alex*	.	*0*	”
2	The Picture	*Alex*	*Bob*	*1*	*02/01/0000 09:00:00*
2	*ETH*	*Bob*	*Alex*	*100*	”
3	The Picture	*Bob*	*Colette*	*1*	*02/01/0000 11:00:00*
3	*ETH*	*Colette*	*Bob*	*200*	”

Example #3: Non-Fungible Tokens

So what actually is an NFT?

Token *= a representation of something (e.g. movie ticket = right to legitimate entry to screening)*

Non-fungible *= cannot be interchanged for other similar objects*

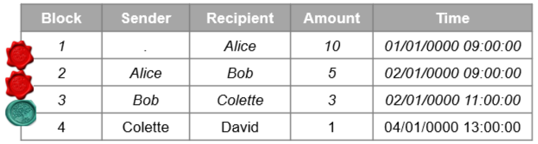
- *Unlike dollars, soybeans or gold*
- *The Mona Lisa, not just any picture or it*
- *My car, not just any version of the same model*

Block	Asset	Sender	Recipient	Amount	Time
1	The Picture	.	*Alex*	*1*	*01/01/0000 09:00:00*
1	*ETH*	*Alex*	.	*0*	”
2	The Picture	*Alex*	*Bob*	*1*	*02/01/0000 09:00:00*
2	*ETH*	*Bob*	*Alex*	*100*	”
3	The Picture	*Bob*	*Colette*	*1*	*02/01/0000 11:00:00*
3	*ETH*	*Colette*	*Bob*	*200*	”

‘A unique digital identifier that cannot be copied, is not interchangeable, and is recorded on a blockchain to certify authenticity and ownership.’

Takeaways

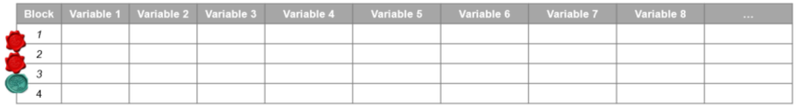
- What is a blockchain?
  - **Spreadsheet rows, securely appended together**



Block	Sender	Recipient	Amount	Time
1	.	*Alice*	*10*	*01/01/0000 09:00:00*
2	*Alice*	*Bob*	*5*	*02/01/0000 09:00:00*
3	*Bob*	*Colette*	*3*	*02/01/0000 11:00:00*
4	Colette	David	1	04/01/0000 13:00:00

- What is Bitcoin?
  - As above**, with particular columns** for tracking ownership of a particular **currency**

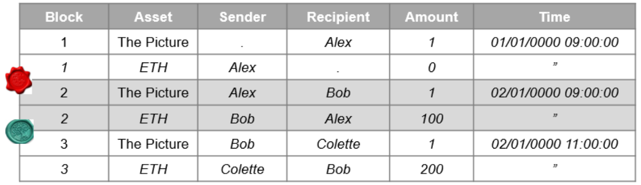
- What is Ethereum?
  - As above**, with flexible column options** and the possibility of using many **formulae**



Block	Variable 1	Variable 2	Variable 3	Variable 4	Variable 5	Variable 6	Variable 7	Variable 8	...
1									
2									
3									
4									

- What is DeFi?
  - **Combinations** of many of the above, to perform more complex financial services

- What are NFTs?
  - As above, **with particular columns** for tracking ownership of specific, **non-swappable assets**



Block	Asset	Sender	Recipient	Amount	Time
1	The Picture	.	*Alex*	*1*	*01/01/0000 09:00:00*
1	*ETH*	*Alex*	.	*0*	”
2	The Picture	*Alex*	*Bob*	*1*	*02/01/0000 09:00:00*
2	*ETH*	*Bob*	*Alex*	*100*	”
3	The Picture	*Bob*	*Colette*	*1*	*02/01/0000 11:00:00*
3	*ETH*	*Colette*	*Bob*	*200*	”