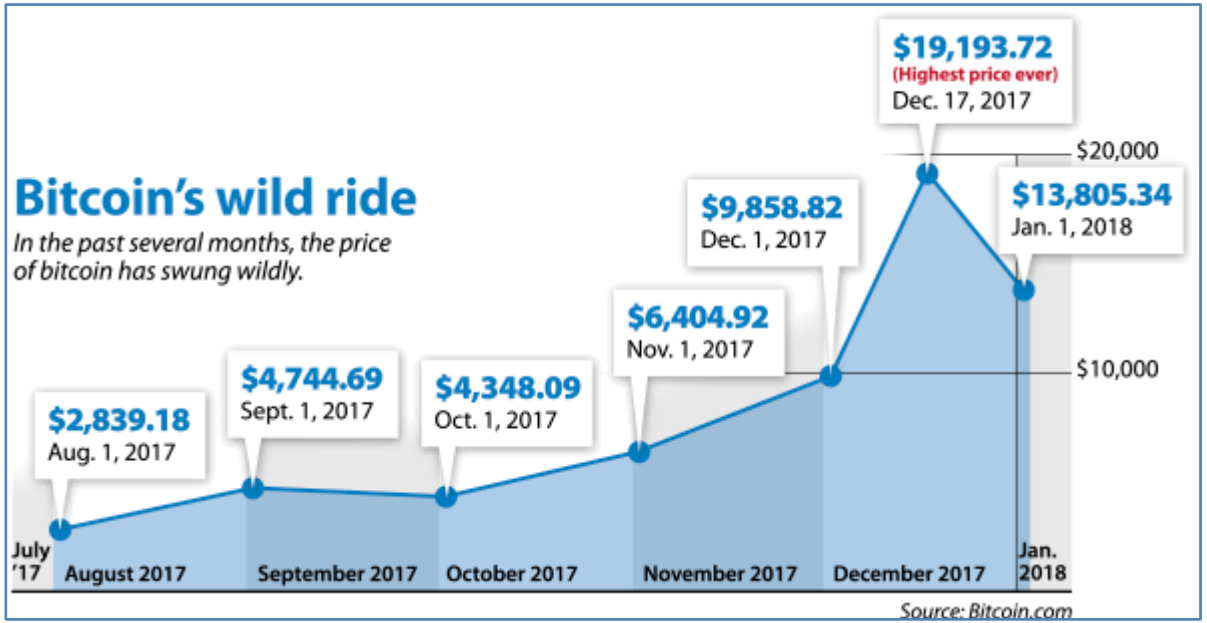
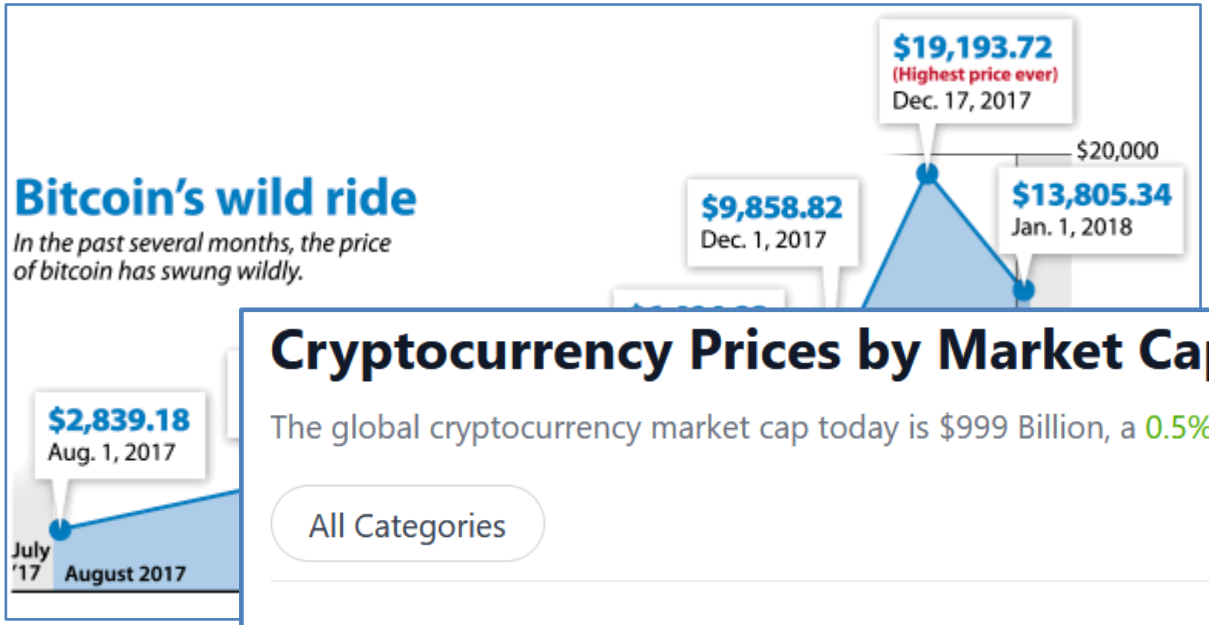
Introduction

How Bitcoin works?

Hype


Bitcoin's wild ride
In the past several months, the price of bitcoin has swung wildly.
$2,839.18
Aug. 1, 2017
$4,744.69
Sept. 1, 2017
$4,348.09
Oct. 1, 2017
$6,404.92
Nov. 1, 2017
$9,858.82
Dec. 1, 2017
$19,193.72
(Highest price ever)
Dec. 17, 2017
$13,805.34
Jan. 1, 2018
$20,000
$10,000
July '17
August 2017
September 2017
October 2017
November 2017
December 2017
Jan. 2018
Source: Bitcoin.com

Hype



Cryptocurrency Prices by Market Cap

Show Stats

The global cryptocurrency market cap today is $999 Billion, a 0.5% change in the last 24 hours.

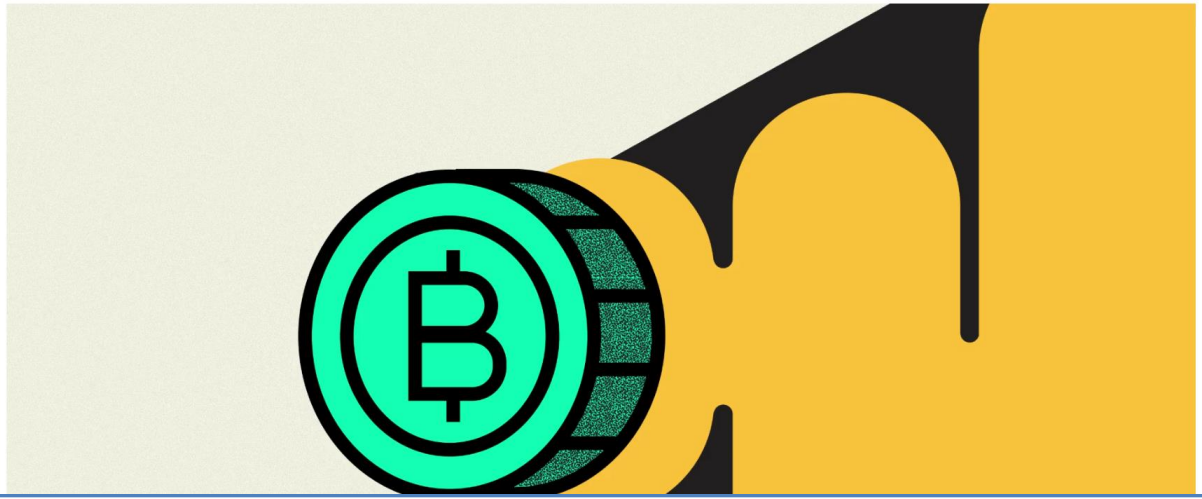
All Categories

#	Coin		Price
☆ 1	Bitcoin BTC	Buy	$20,133.20

Hype

WIRED Bitcoin Will Burn the Planet Down. The Question: How Fast? SIGN IN

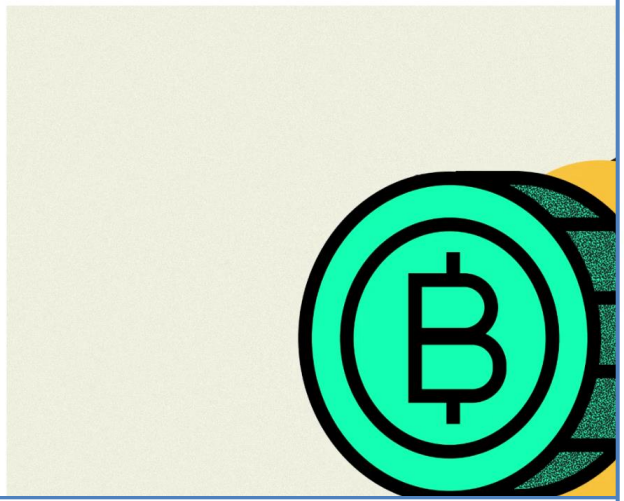
BITCOIN WILL BURN THE PLANET DOWN. THE QUESTION: HOW FAST?



Hype

WIRED Bitcoin Will Burn the Planet Down. The Question: How Fast? SIGN IN

BITCOIN WILL BURN THE PLANET DOWN. THE QUESTION: HOW FAST?



'Bitcoin will die as a complete load of nonsense' says Ardo Hansson

07 JAN, 2019 | UPDATED: 07 JAN, 2019 BY JOERI CANT

NEWS

Hype

WIRED Bitcoin Will Burn the Planet Down. The Question: How Fast? SIGN IN

BITCOIN WILL BURN THE PLANET DOWN. THE QUESTION: HOW FAST?

https://99bitcoins.com/bitcoin-obituaries/

99BITCOINS BUY & TRADE GET A WALLET EXCHANGE REVIEWS

Bitcoin Obituaries

Bitcoin has died 345 times

Submit an Obituary

Hype

Apple co-founder believes Bitcoin will transform the world

October 27, 2018

17980

Facebook | Twitter | Pinterest | Linkedin

Apple co-founder Steve Wozniak

Hype

Apple co-founder believes Bitcoin will transform the world

October 27, 2018

17980

Facebook | Twitter | Pinterest | Link

Apple co-founder Steve Wozniak

MONEYWEEK
The UK's best-selling financial magazine

Try 6 free issues »

Home | Investments | Prices & Charts | Trading | Gold | Economy | Pers. Finance

Hot topics | Isas | Cryptocurrencies | House prices | Brexit | Tech stocks | Inves

Home > Currencies > Bitcoin will change the world forever

Bitcoin will change the world forever

Legend

Bitcoin is the first cryptocurrency

ACC	CyberCents	iKP	MPTP	Proton
Agora	CyberCoin	IMB-MP	Net900	Redi-Charge
AIMP	CyberGold	InterCoin	NetBill	S/PAY
Allopass	DigiGold	Ipin	NetCard	Sandia Lab E-Cash
b-money	Digital Silk Road	Javien	NetCash	Secure Courier
BankNet	e-Comm	Karma	NetCheque	Semopo
Bitbit	E-Gold	LotteryTickets	NetFare	SET
Bitgold	Ecash	Lucre	No3rd	SET2Go
Bitpass	eCharge	MagicMoney	One Click Charge	SubScrip
C-SET	eCoin	Mandate	PayMe	Trivnet
CAFÉ	Edd	MicroMint	PayNet	TUB
CheckFree	eVend	Micromoney	PayPal	Twitpay
ClickandBuy	First Virtual	MilliCent	PaySafeCard	VeriFone
ClickShare	FSTC Electronic Check	Mini-Pay	PayTrust	VisaCash
CommerceNet	Geldkarte	Minitix	PayWord	Wallie
CommercePOINT	Globe Left	MobileMoney	Peppercoin	Way2Pay
CommerceSTAGE	Hashcash	Mojo	PhoneTicks	WorldPay
Cybank	HINDE	Mollie	Playspan	X-Pay
CyberCash	iBill	Mondex	Polling	

Table 1: Notable electronic payment systems and proposals

Legend

Bitcoin is the first cryptocurrency

ACC	CyberCents	iKP	MPTP	Proton
Agora	CyberCoin	IMB-MP	Net900	Redi-Charge
AIMP	CyberGold	InterCoin	NetBill	S/PAY
Allopass	DigiGold	Ipin	NetCard	Sandia Lab E-Cash
b-money	Digital Silk Road	Javien	NetCash	Secure Courier
BankNet	e-Comm	Karma	NetCheque	Semopo
Bitbit	E-Gold	LotteryTickets	NetFare	SET
Bitgold	Ecash	Lucre	No3rd	SET2Go
Bitpass	eCharge	MagicMoney	One Click Charge	SubScrip
C-SET	eCoin	Mandate	PayMe	Trivnet
CAFÉ	Edd	MicroMint	PayNet	TUB
CheckFree	eVend	Micromoney	PayPal	Twitpay
ClickandBuy	First Virtual	MilliCent	PaySafeCard	VeriFone
ClickShare	FSTC Electronic Check	Mini-Pay	PayTrust	VisaCash
CommerceNet	Geldkarte	Minitix	PayWord	Wallie
CommercePOINT	Globe Left	MobileMoney	Peppercoin	Way2Pay
CommerceSTAGE	Hashcash	Mojo	PhoneTicks	WorldPay
Cybank	HINDE	Mollie	Playspan	X-Pay
CyberCash	iBill	Mondex	Polling	

Table 1: Notable electronic payment systems and proposals

Mystery

Satoshi Nakamoto

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Mystery

Satoshi Nakamoto

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

What is Bitcoin?

- Money for the internet
- An electronic form of money
- Money of the future

What is Bitcoin?

- Money for the internet
- An electronic form of money
- Money of the future

What is money?

Exchange of goods

Alice

Bob

Exchange of goods

Alice

Bob

Exchange of goods

Alice

Bob

Exchange of goods

Alice

I need vegetables!

Bob

Exchange of goods

Alice

I need vegetables!

Bob

I need fish!

Exchange of goods

Alice

Let’s exchange products.

Bob

Let’s exchange products.

Exchange of goods

Alice

Bob

Exchange of goods

Alice

Bob

Exchange of goods

Alice

Bob

Exchange of goods

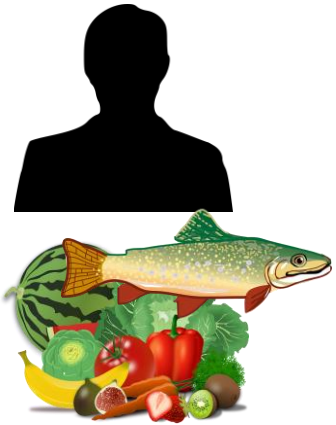
Alice

Bob

Exchange of goods

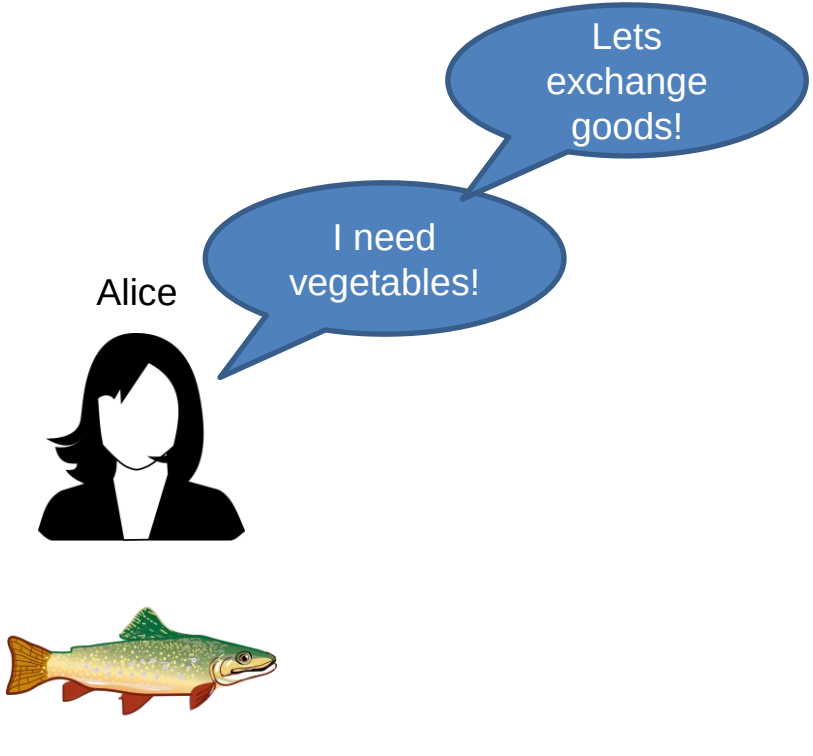
Alice

Bob



Exchange of goods

Exchange of goods



Exchange of goods

Alice

Lets exchange goods!

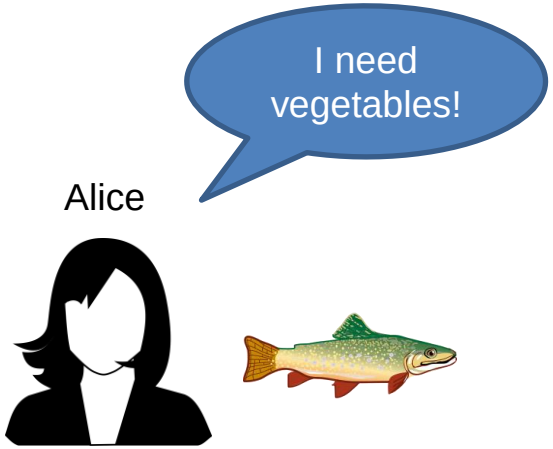
I need vegetables!

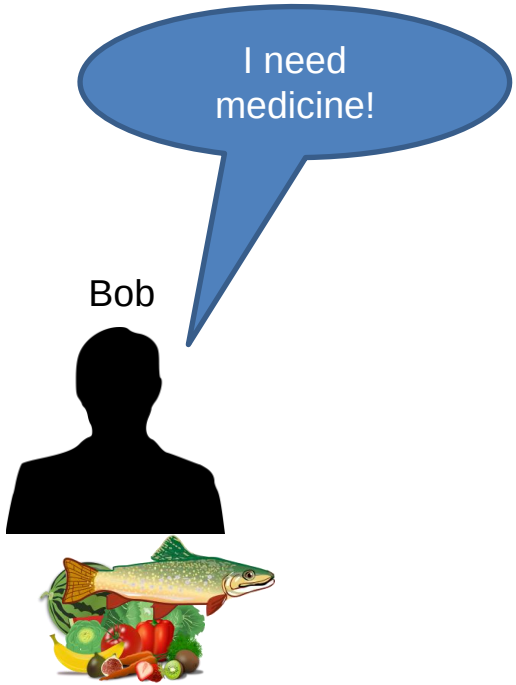
Bob

But I do need medicine!

Sorry, I don't need fish!

Exchange of goods





Exchange of goods

I need vegetables!

Alice

I need medicine!

Bob

Charlie

Exchange of goods

I need vegetables!

Alice

I need medicine!

Bob

Charlie

Exchange of goods

I need vegetables!

Alice

I need medicine!

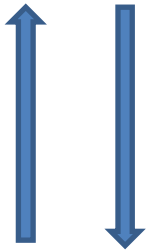
Bob

I need fish!

Charlie

Exchange of goods

Alice

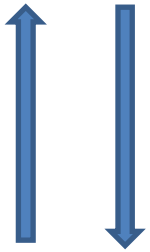


Charlie

Bob

Exchange of goods

Alice

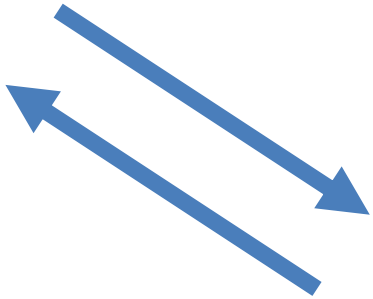


Charlie

Bob

Exchange of goods

Alice

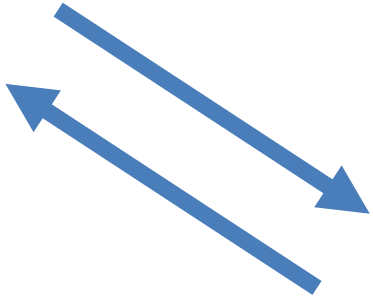


Bob

Charlie

Exchange of goods

Alice



Bob

Charlie

What’s the issue?

- Kind of complicated!!!
- How to coordinate all the exchanges?
- What is a Good solution for this?

Traditional money (cash)

Alice

Bob

Traditional money (cash)

Alice

Bob

Traditional money (cash)

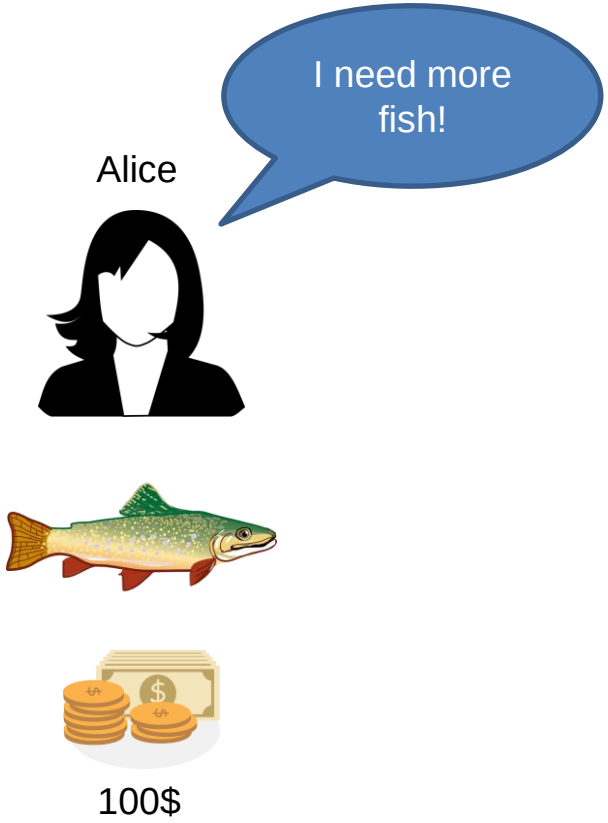
Alice

100$

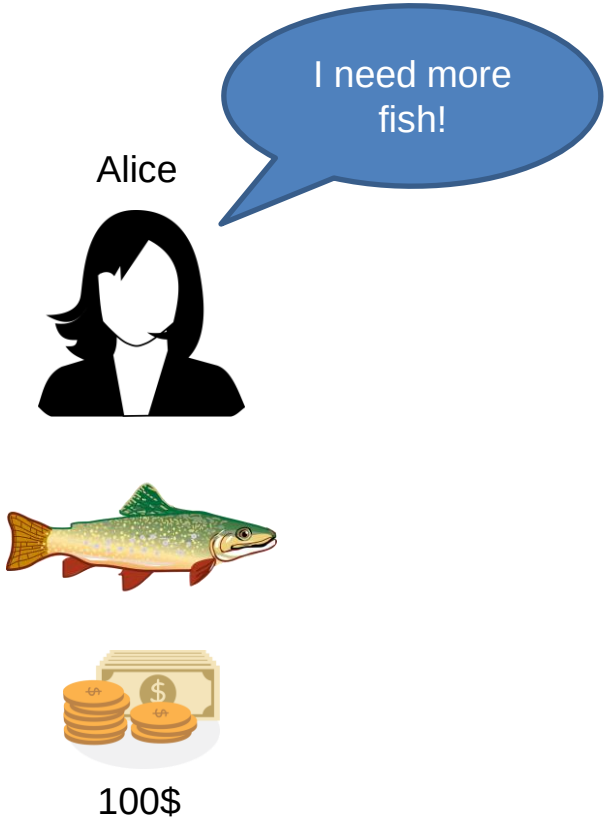
Bob

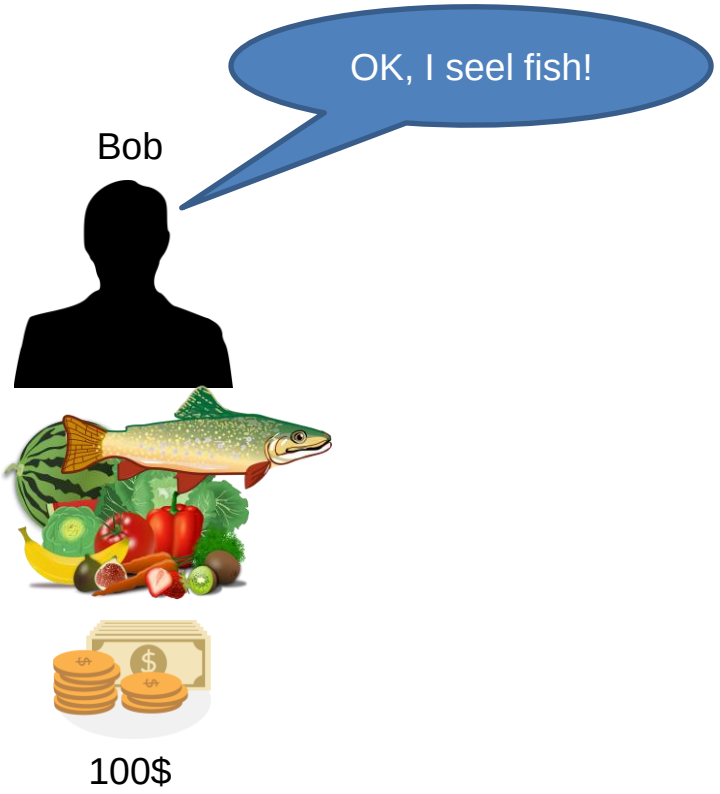
100$

Traditional money (cash)

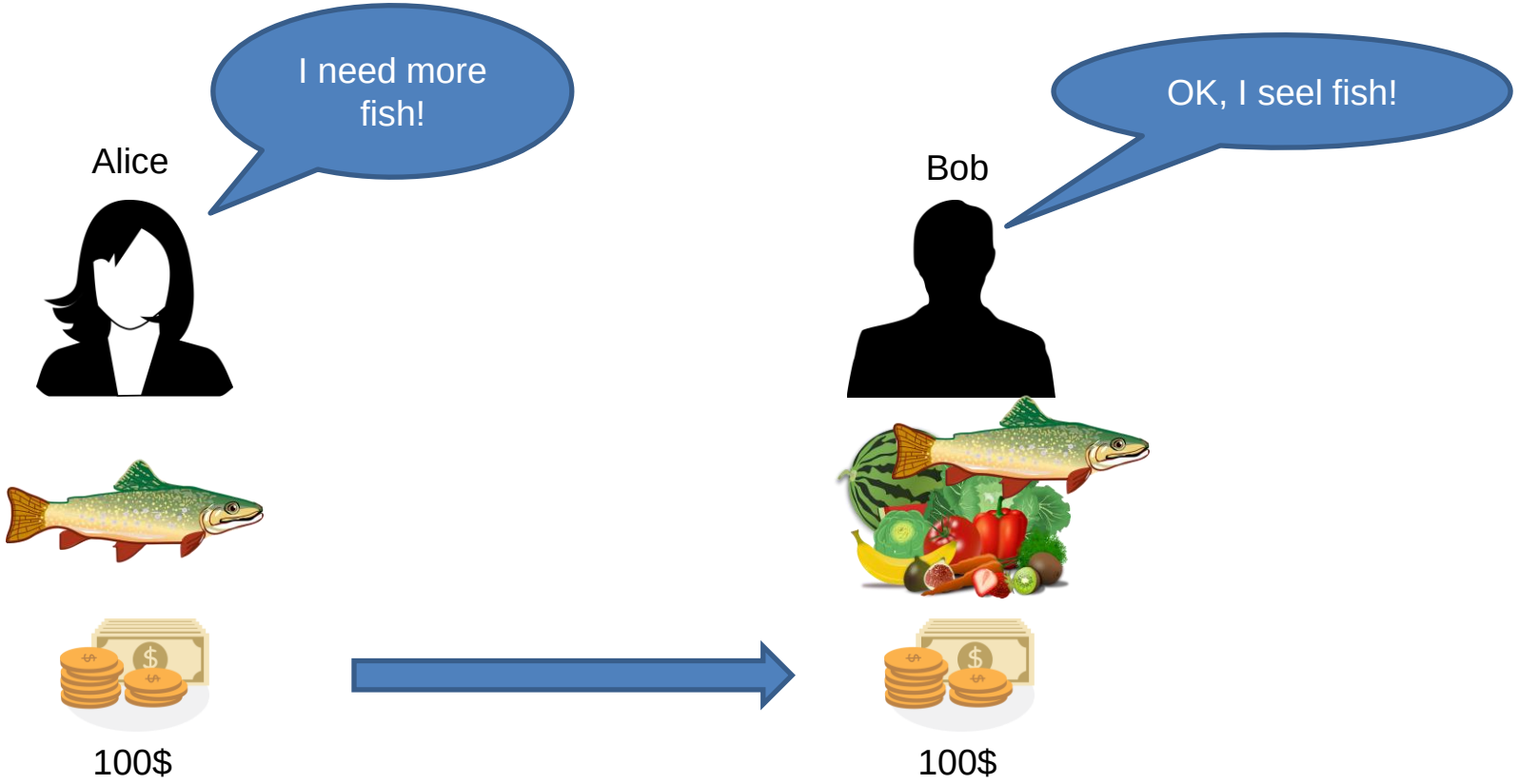


Traditional money (cash)

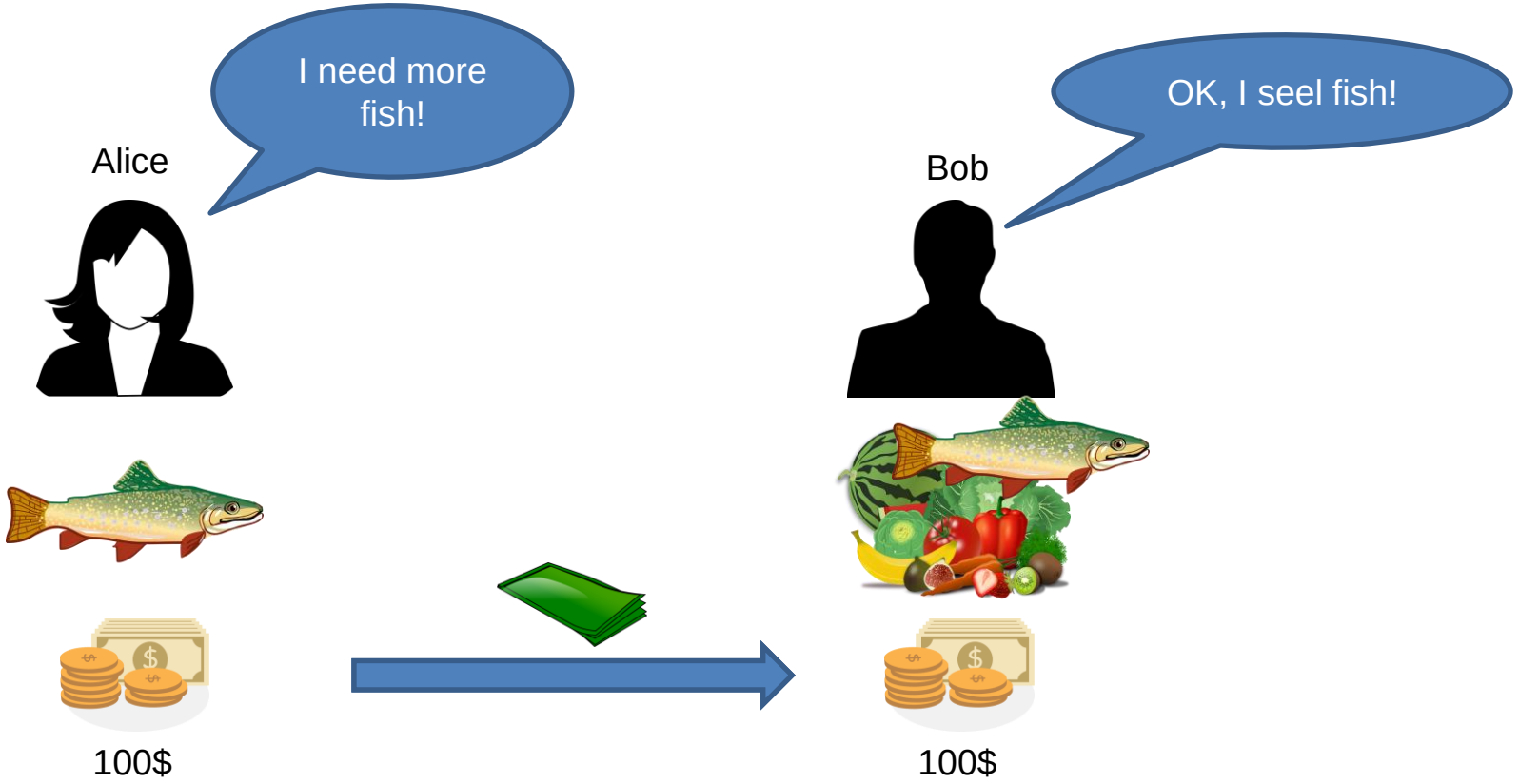




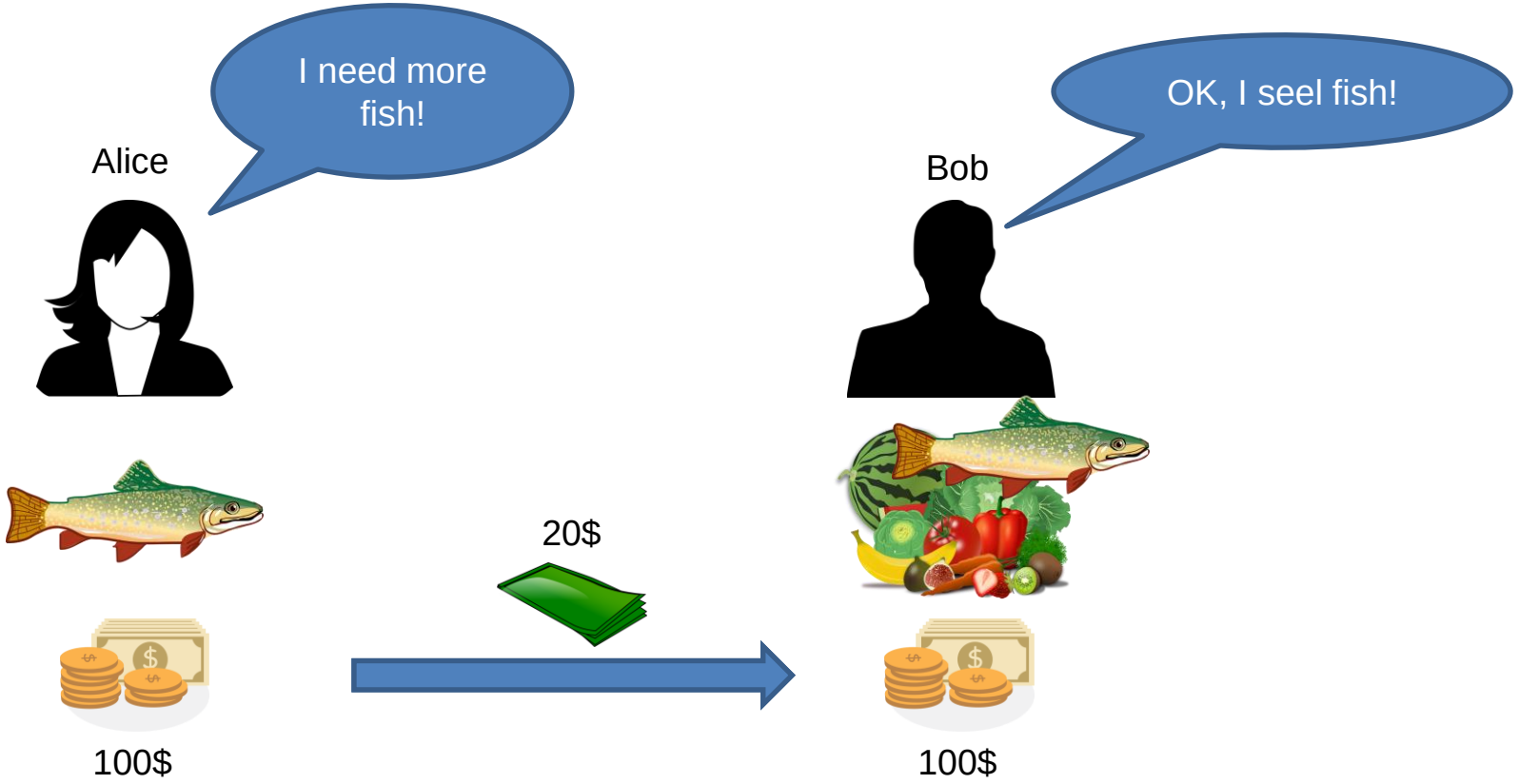
Traditional money (cash)



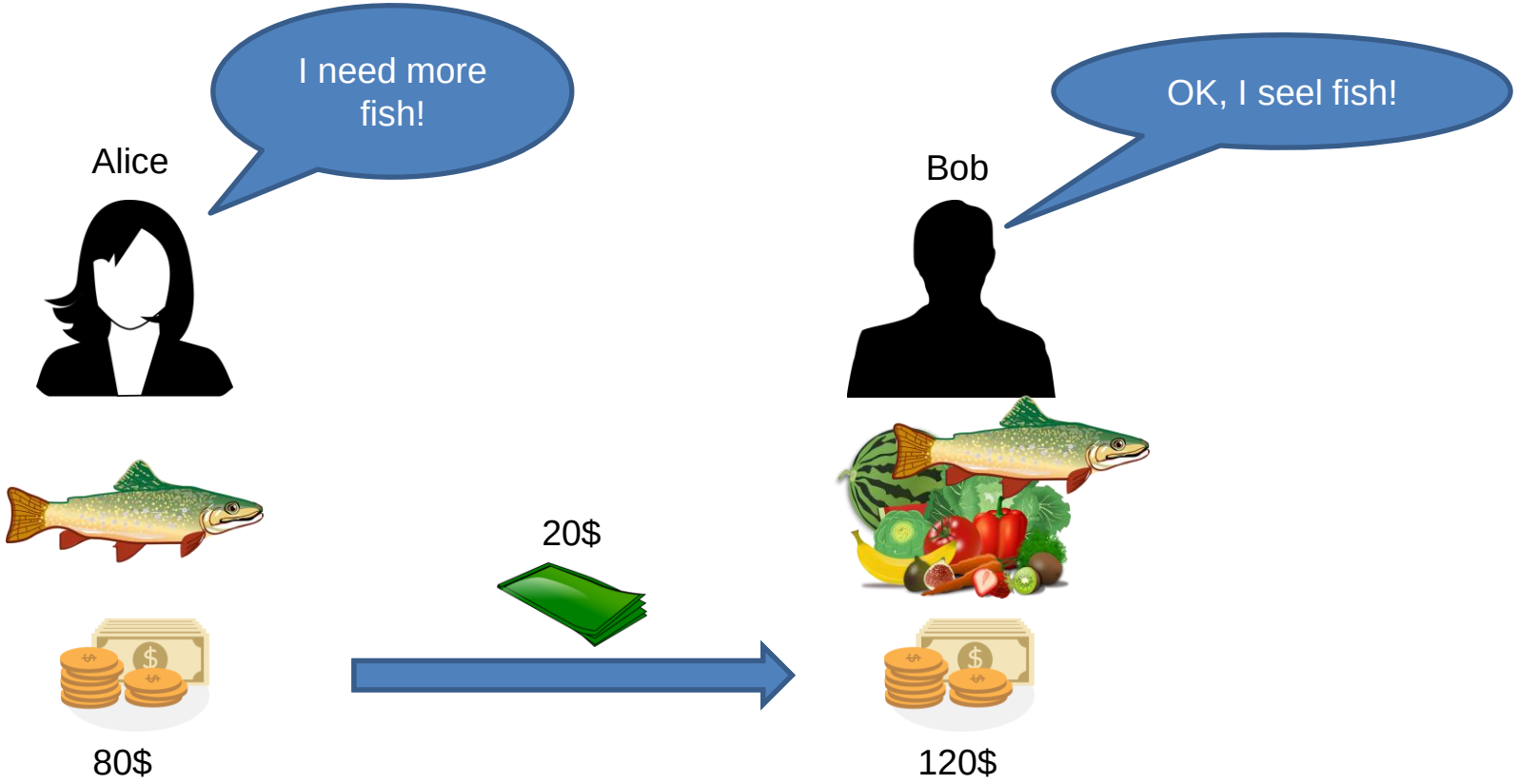
Traditional money (cash)



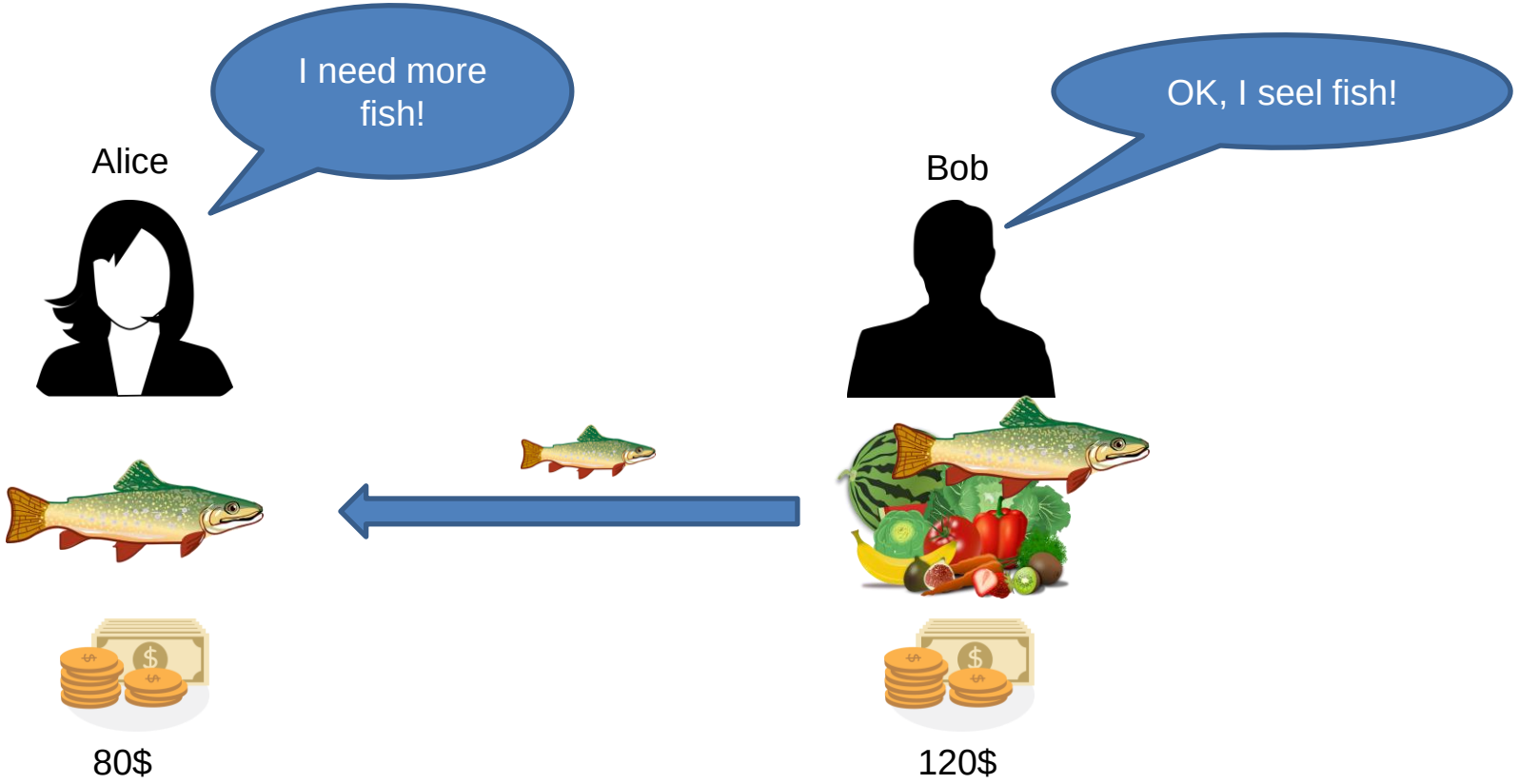
Traditional money (cash)



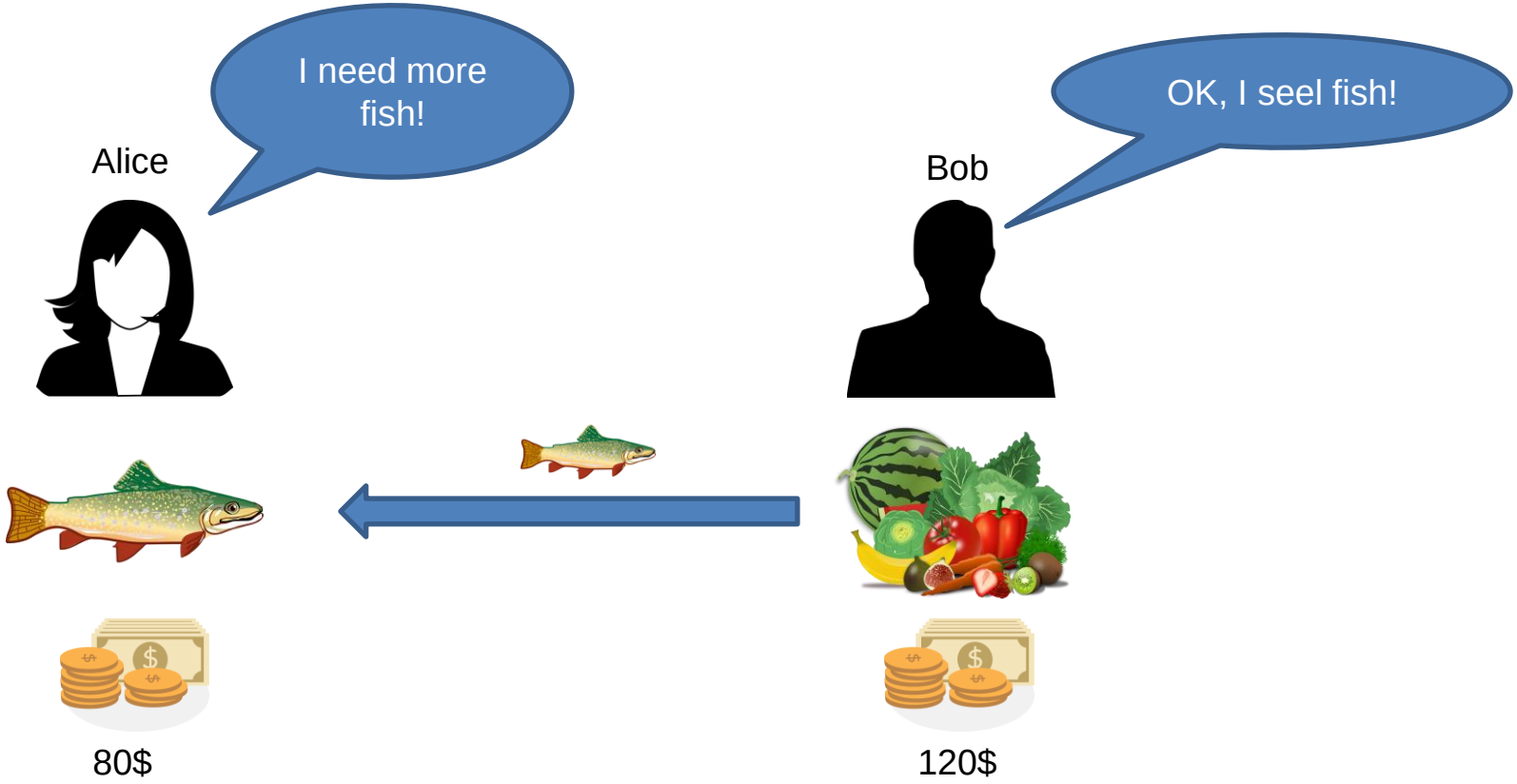
Traditional money (cash)



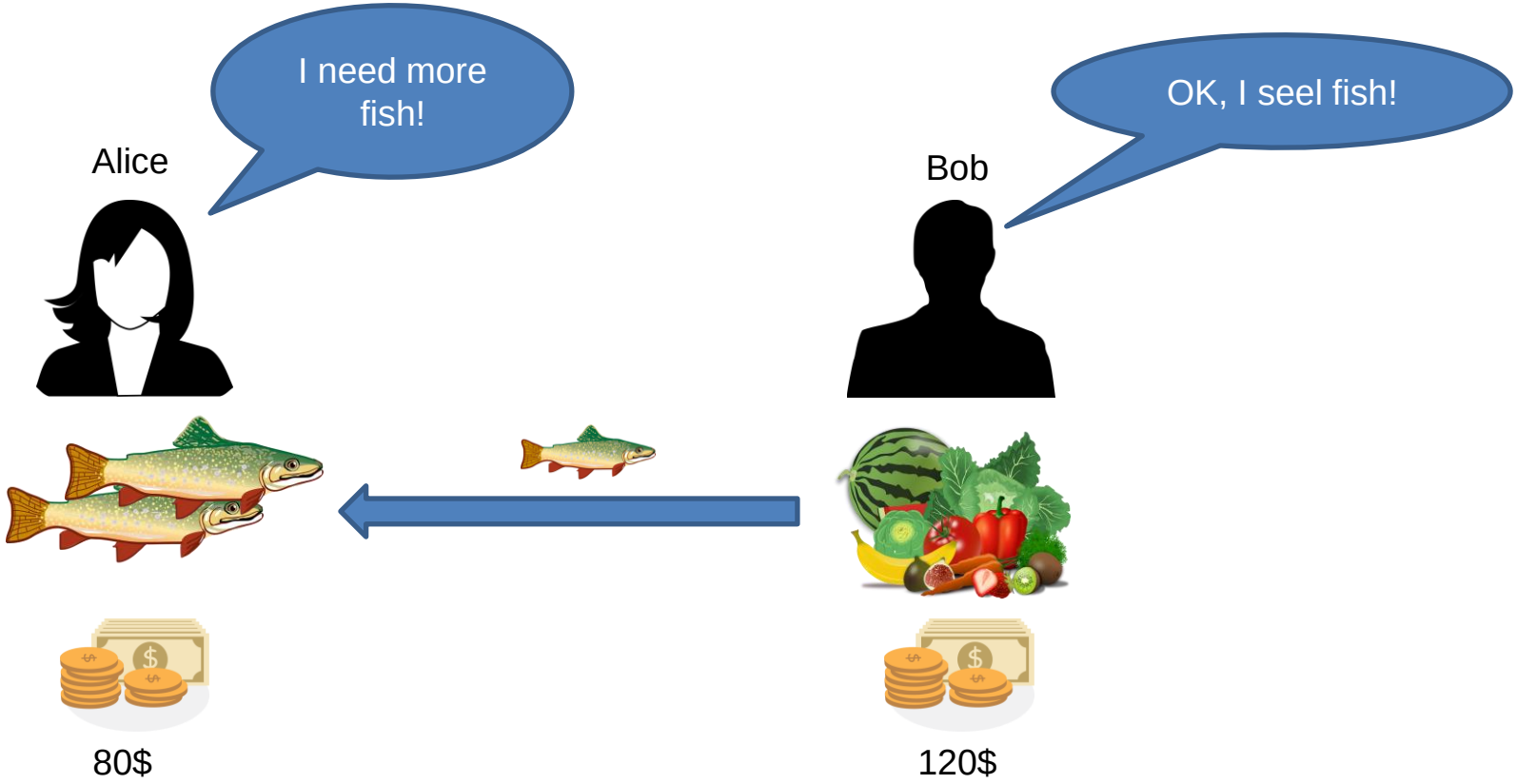
Traditional money (cash)



Traditional money (cash)



Traditional money (cash)



Some questions about cash

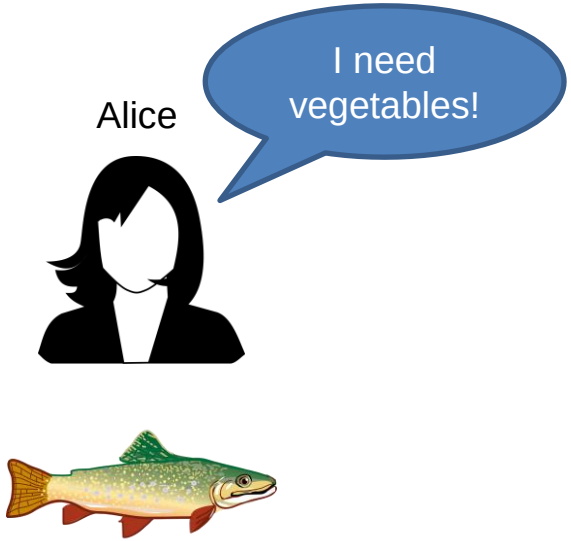
- Where does the cash come from?
- What are the benefits of cash?

Credit

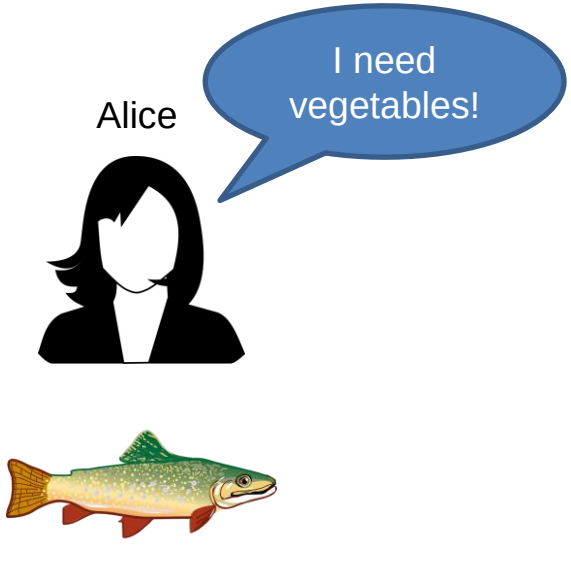
Alice

Bob

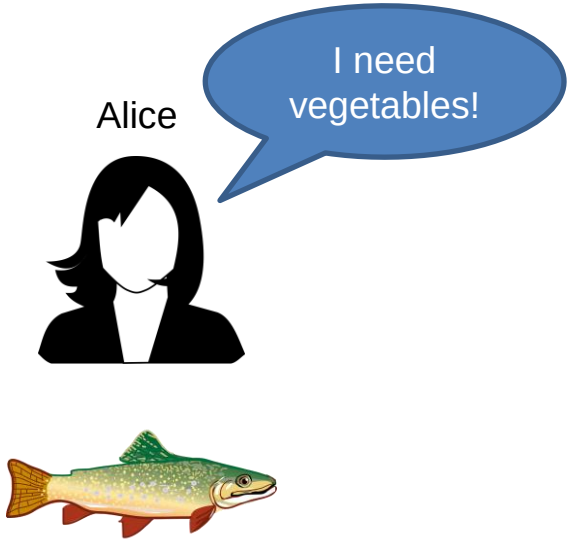
Credit



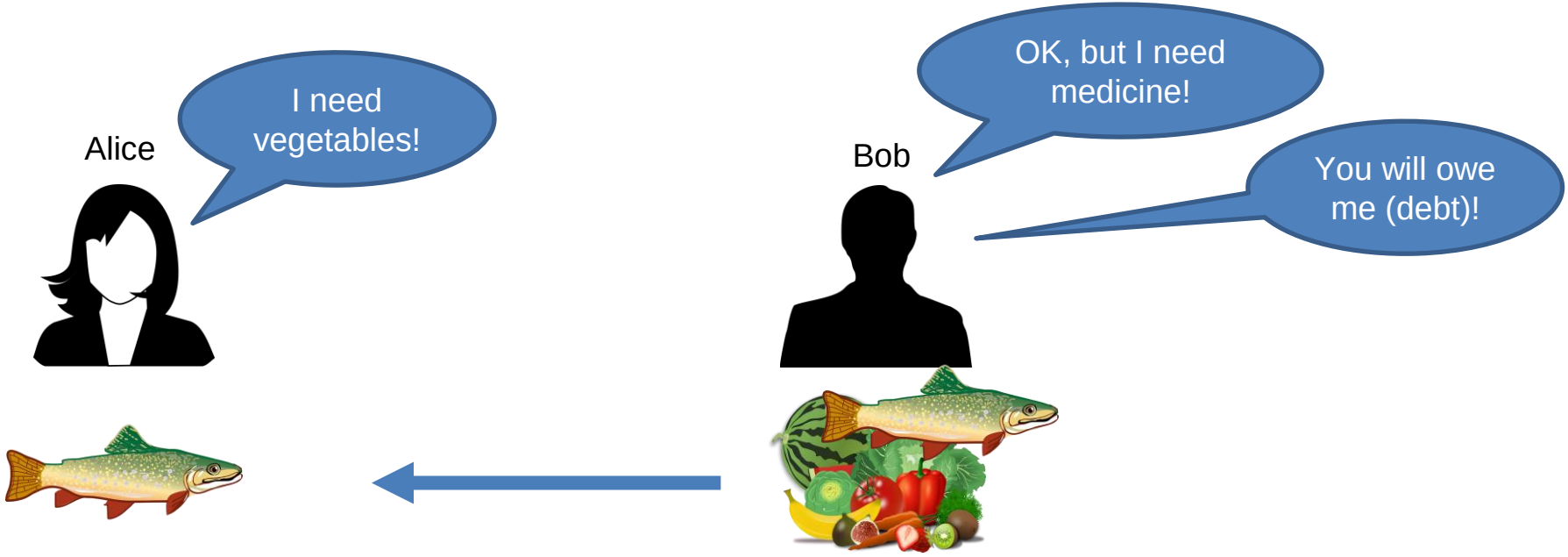
Credit



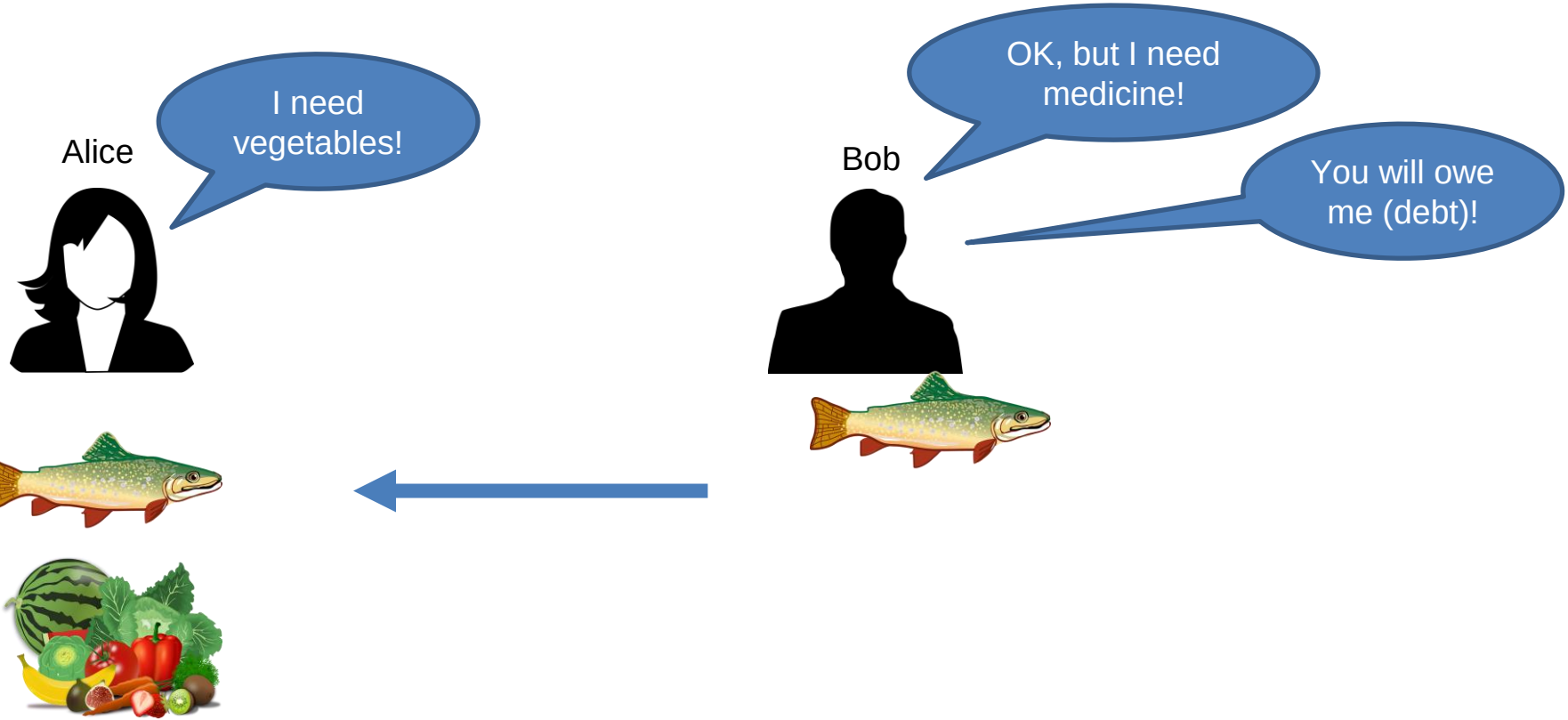
Credit


Alice
I need vegetables!
Bob
OK, but I need medicine!
You will owe me (debt)!

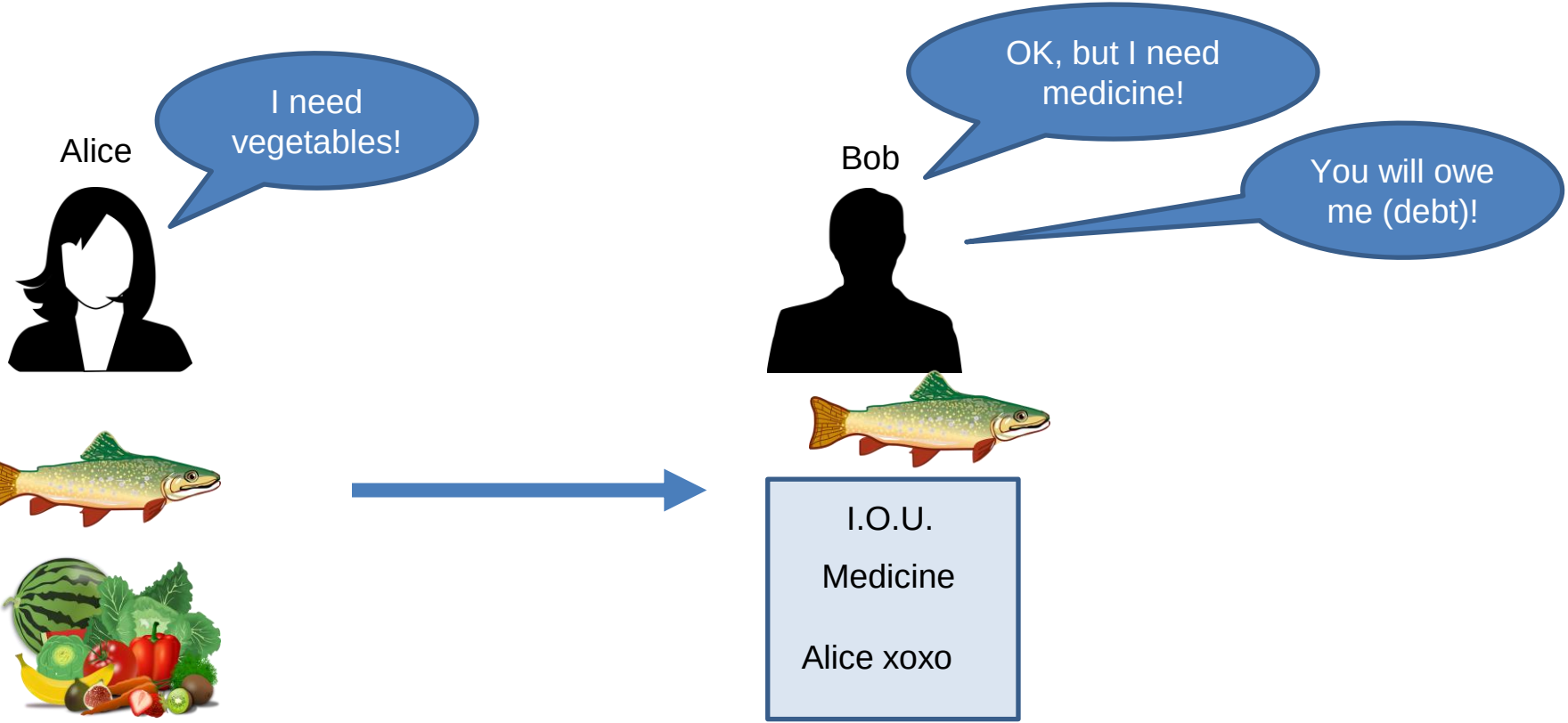
Credit


Alice
I need vegetables!
Bob
OK, but I need medicine!
You will owe me (debt)!

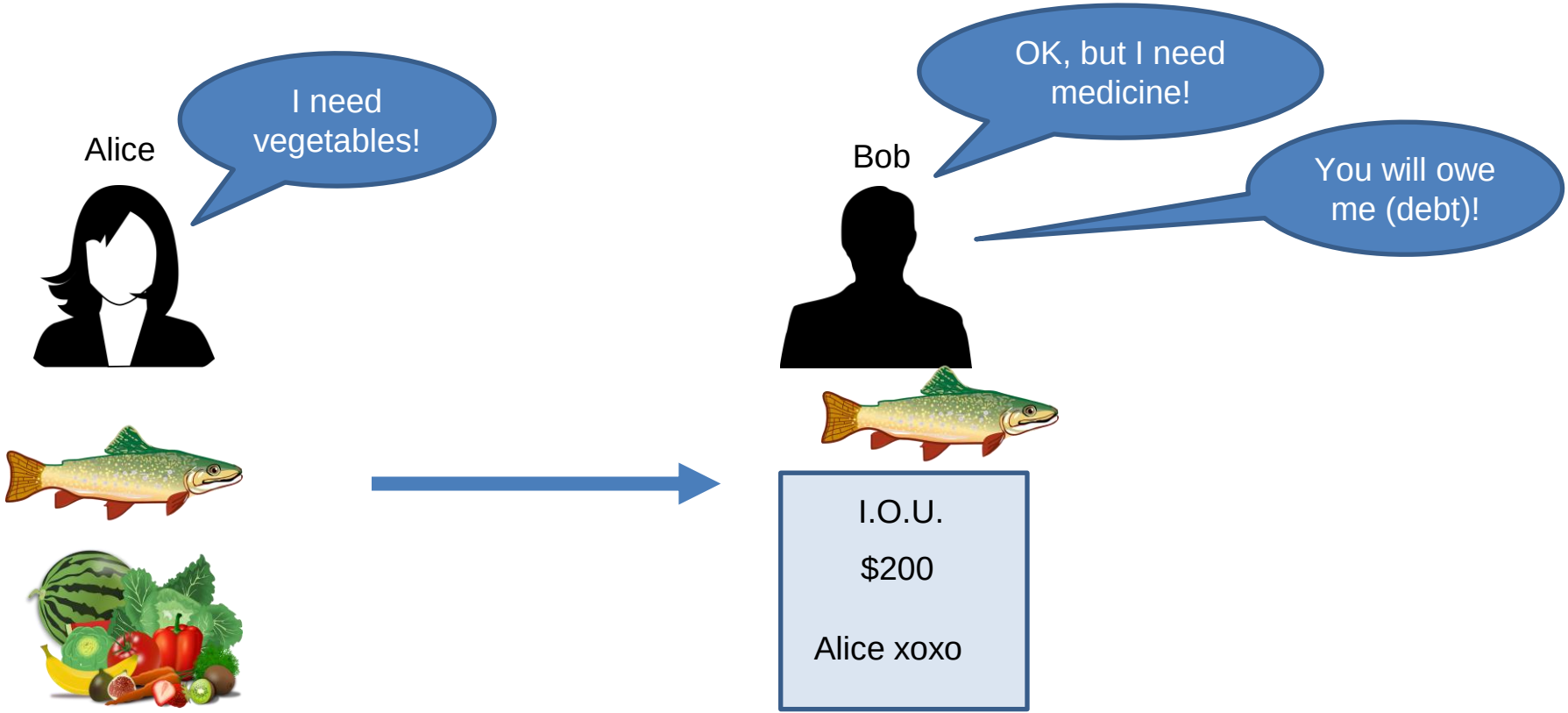
Credit


Alice
I need vegetables!
Bob
OK, but I need medicine!
You will owe me (debt)!

Credit


Alice
I need vegetables!
Bob
OK, but I need medicine!
You will owe me (debt)!
I.O.U.
Medicine
Alice xoxo

Cash credit (hybrid)



Some questions about credit

- What’s the issue with credit?

Examples

- Credit:
  - Credit card
  - Bank loan
- Cash:
  - Cash (kuna, dolar, euro,…)
  - BitCoin

Properties of cash

- Disadvantage:
  - Initial emission (bootstrapping)

- Advantages:
  - Precision
  - You can not escape your debt (unless you are a millionare)
  - Anonimity
  - Fungible
  - Offline transactions

BitCoin as cash

- Emission of BitCoin: mining
- Anonimity: pseudonimity
- Offline transactions: nah/maybe (green addresses)
- Fungibility: not really (pseudonimity)

A characteristis of today’s economy

- Credit card:
  - Bank/PayPal/Visa/Mastercard check all the transactions

- Cash:
  - Emitted by a central bank; series number on each bill

Central entity (bank, government) controls everything

(Why is this good?)

Problem with centralization

- If we want global currency (‘’for the internet”)
  - Who will control everything?
- What does BitCoin propose?
  - Decentralization
  - But it also has some disadvantages

What does the economy look like?

I'll buy fish from Bob!

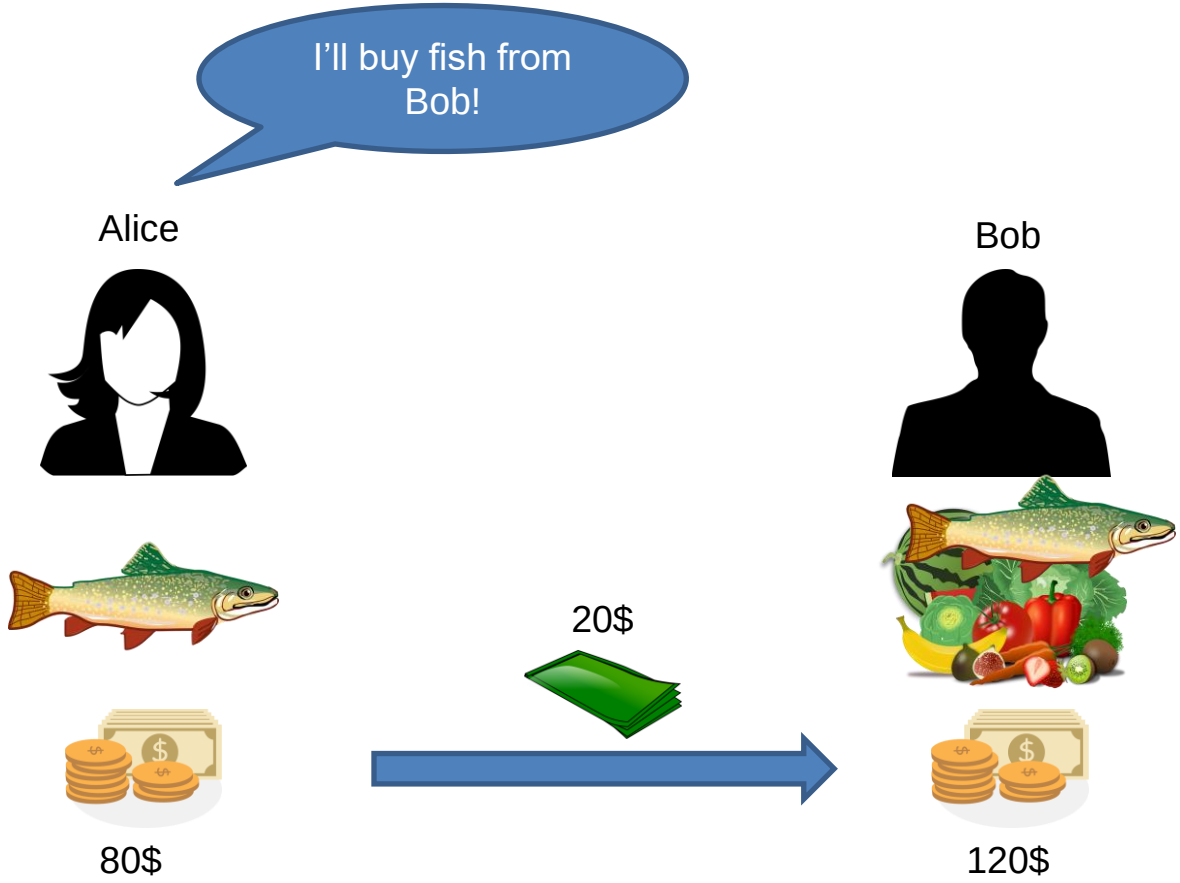
Alice

100$

Bob

100$

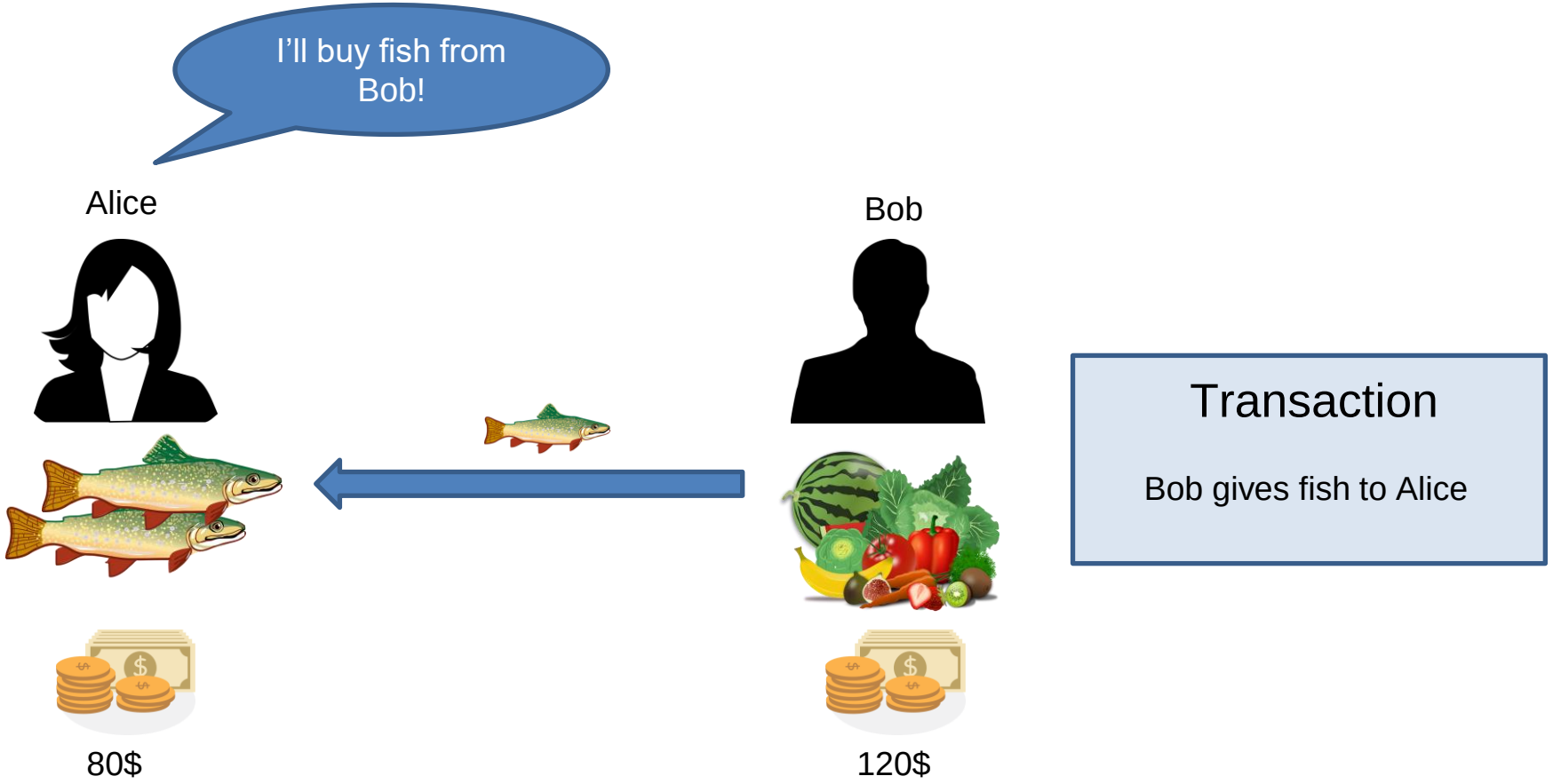
What does the economy look like?



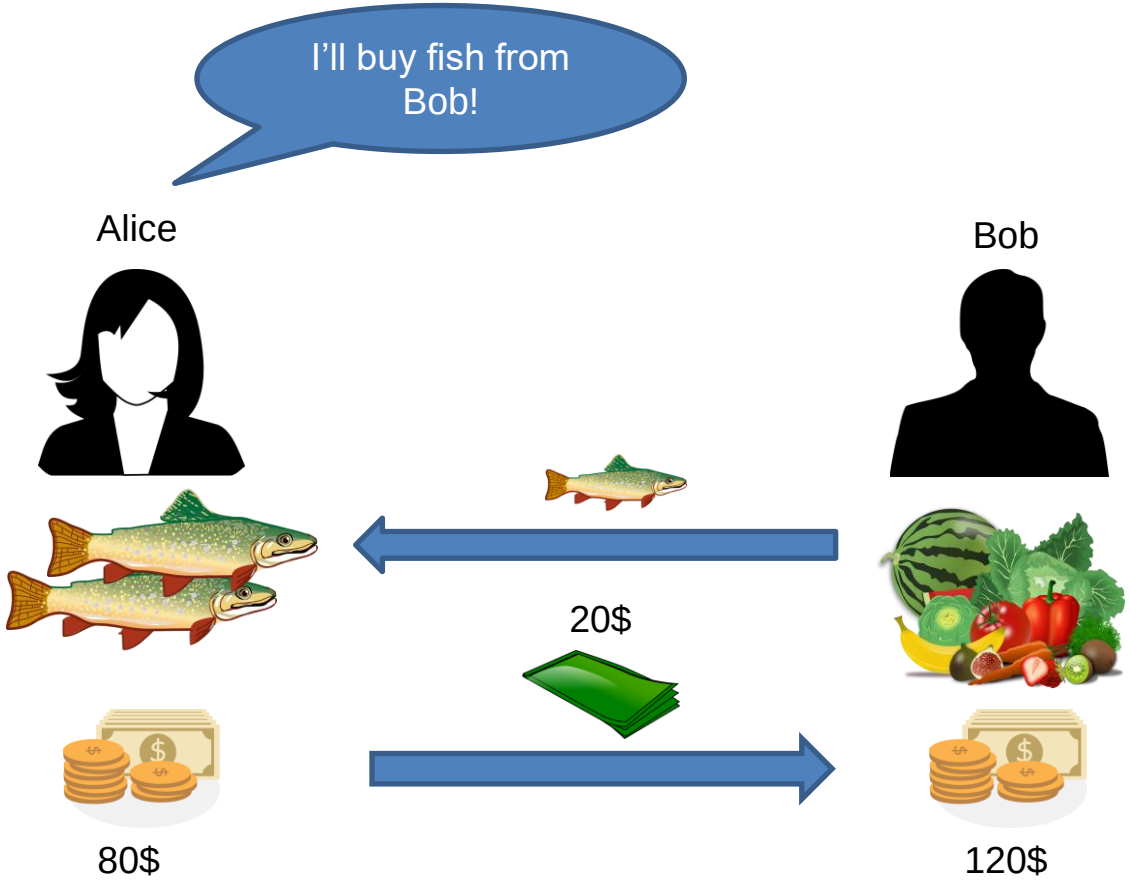
Transaction

Alice pays Bob $20

Atomic unit of economy



Atomic unit of economy



Exchange

Alice pays Bob $20

Bob gives fish to Alice

What does the economy look like?

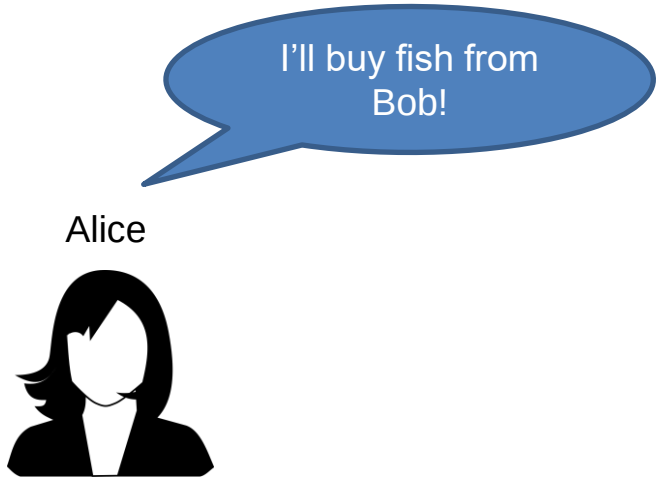
A simple version of economy

Alice

Bob

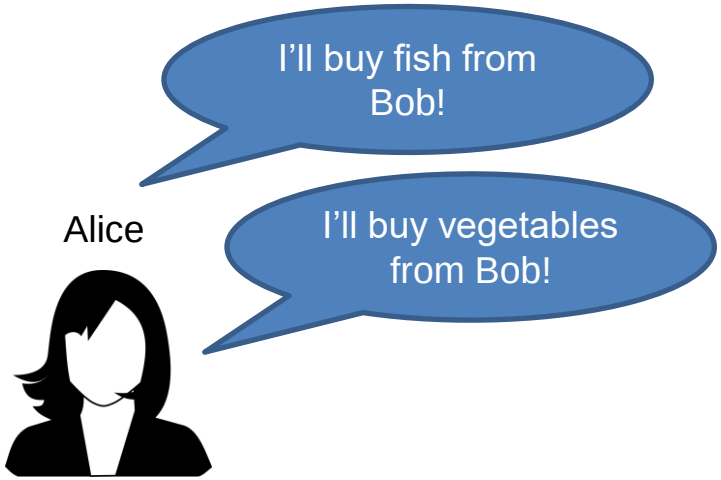
Ledger

A simple version of economy



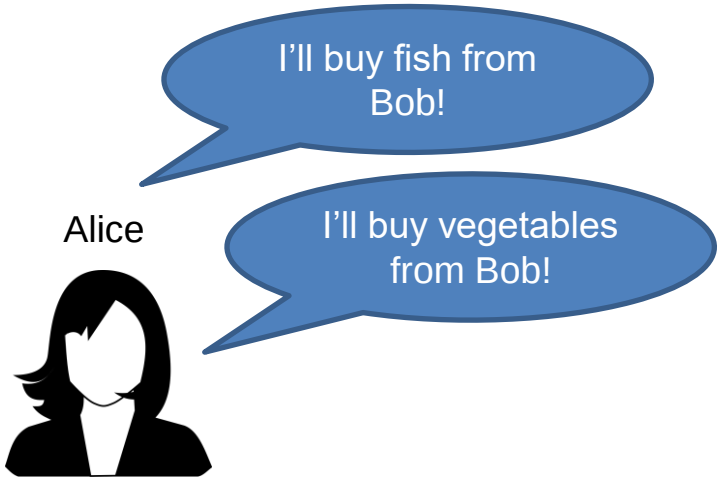
Ledger

A simple version of economy



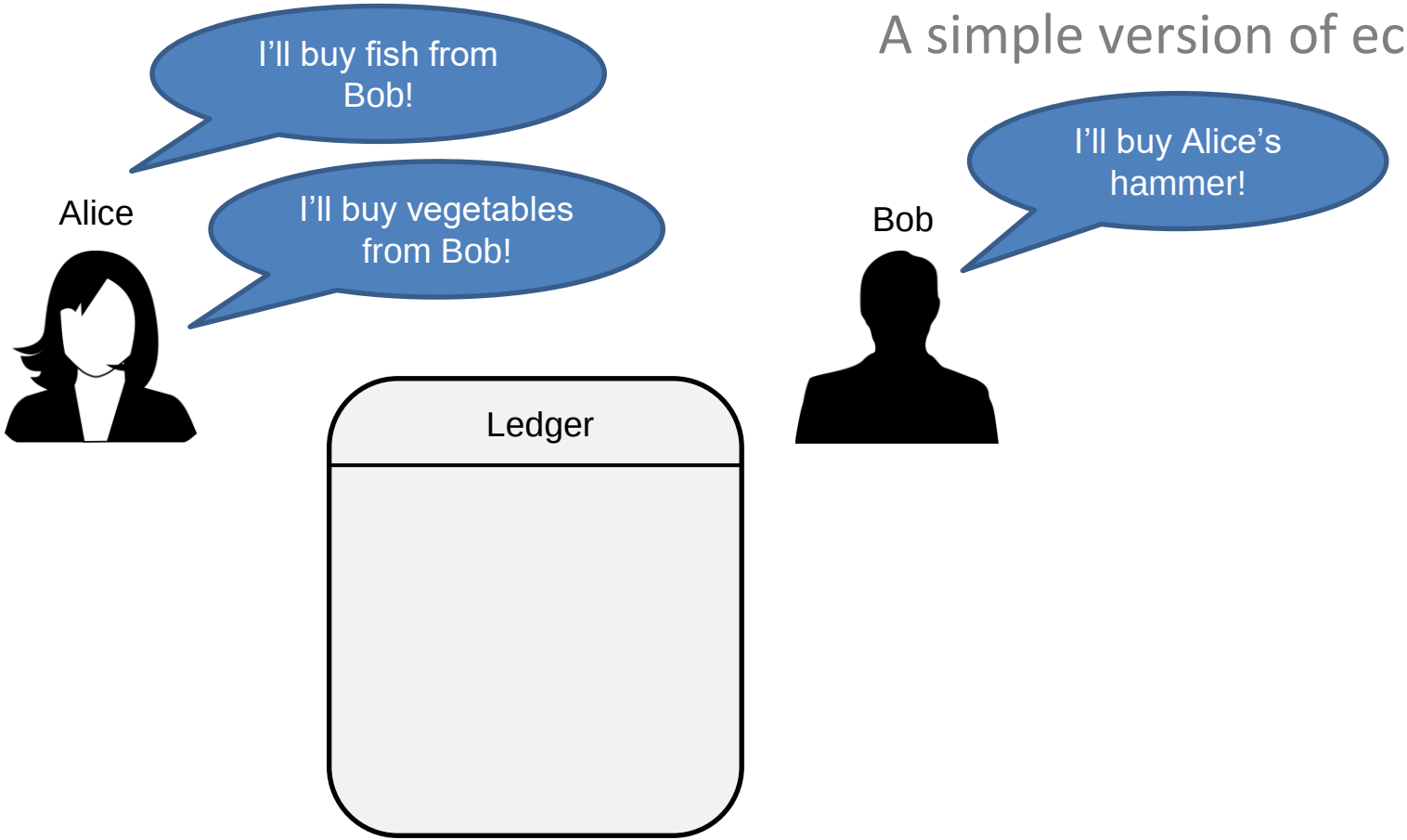
Ledger

A simple version of economy



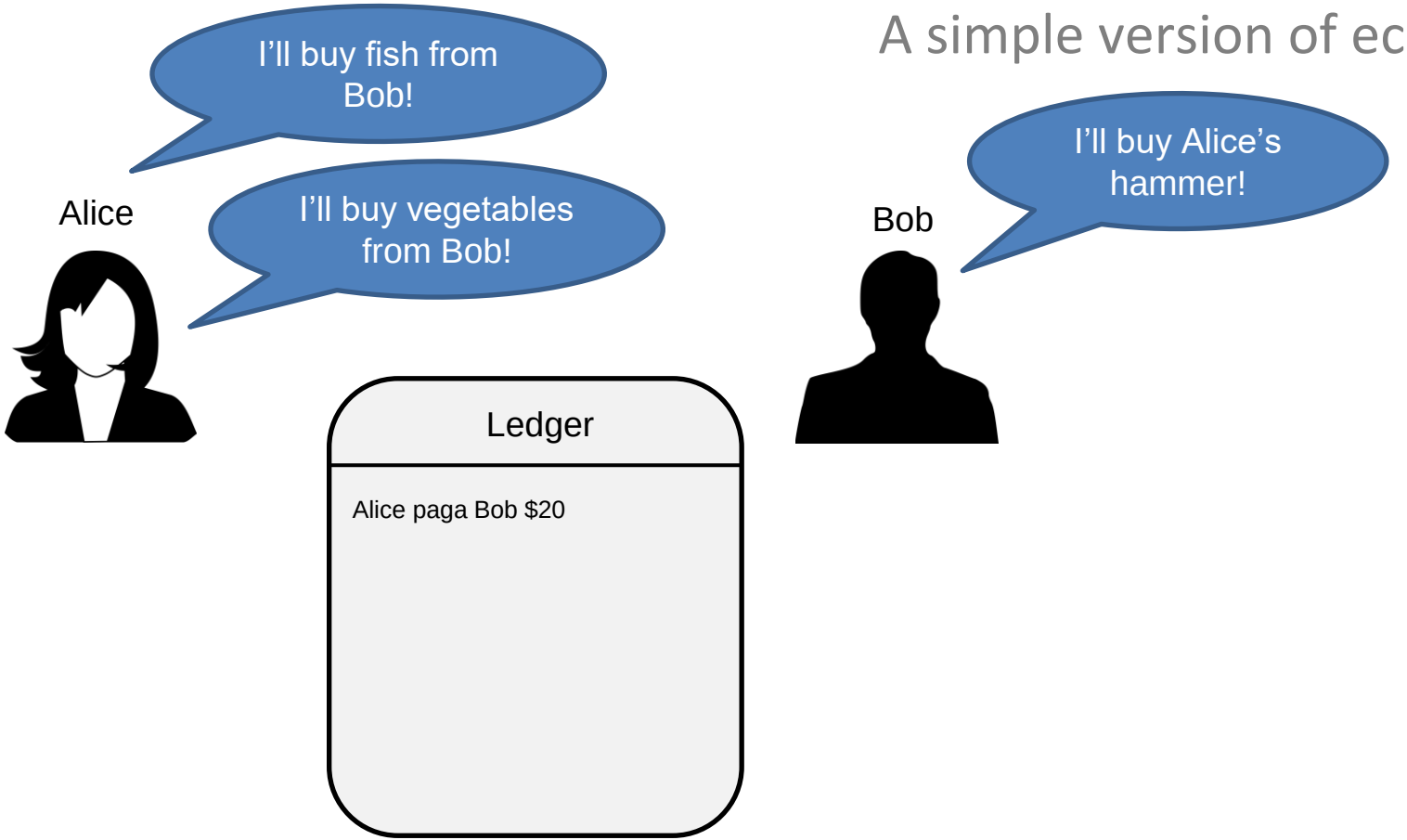
Ledger

A simple version of economy



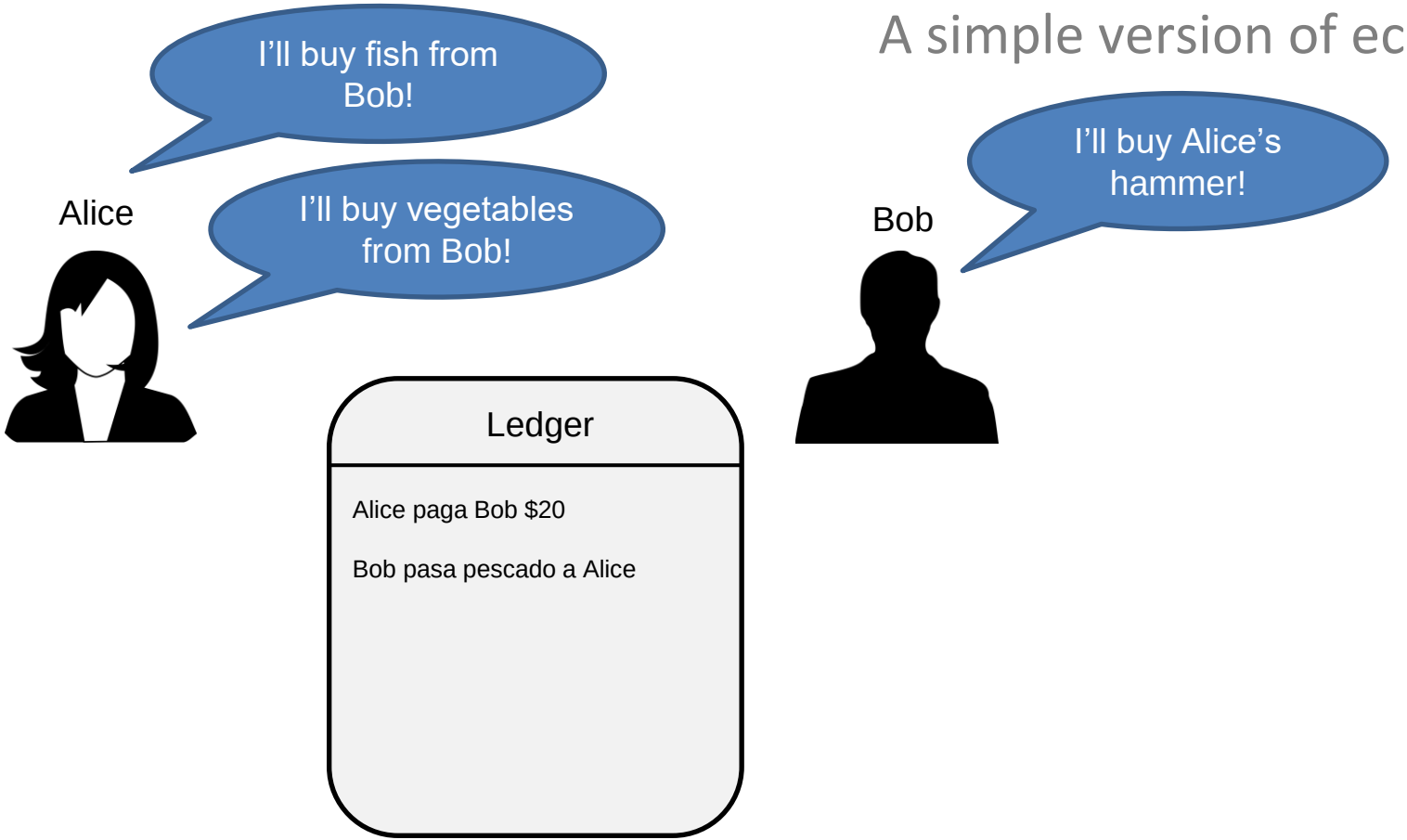
Ledger

A simple version of economy



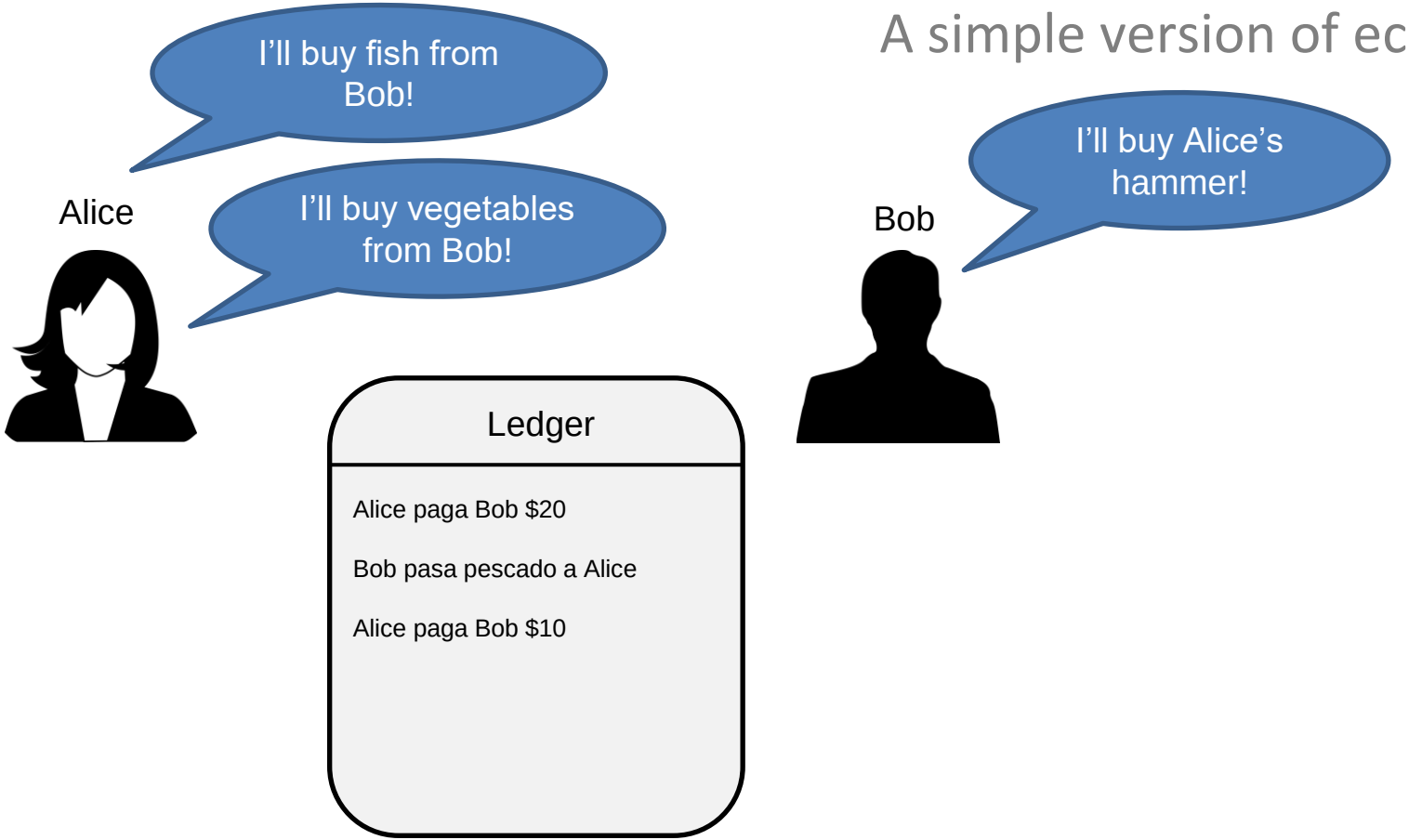
Ledger

A simple version of economy



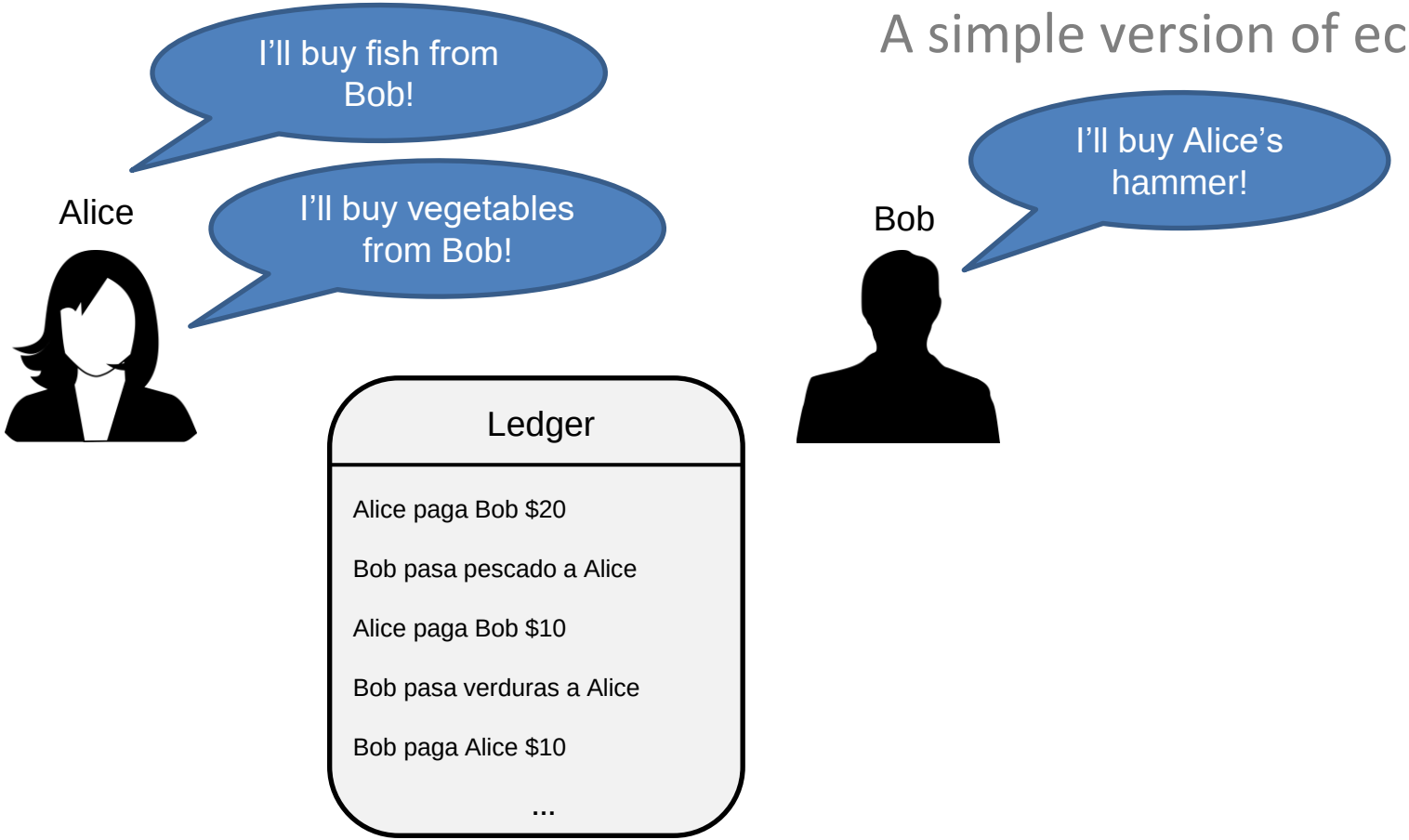
Ledger

A simple version of economy



Ledger

A simple version of economy



Ledger

Alice

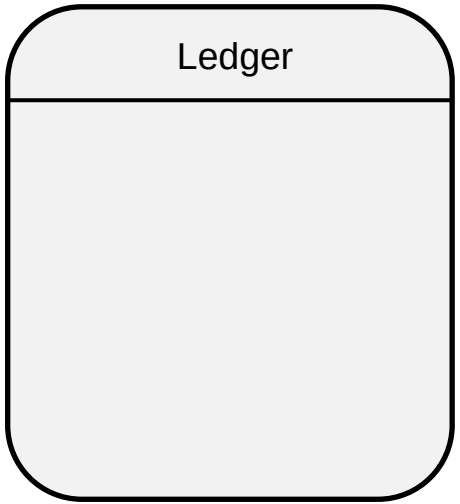
Bob

Charlie

Ledger

Alice

Charlie

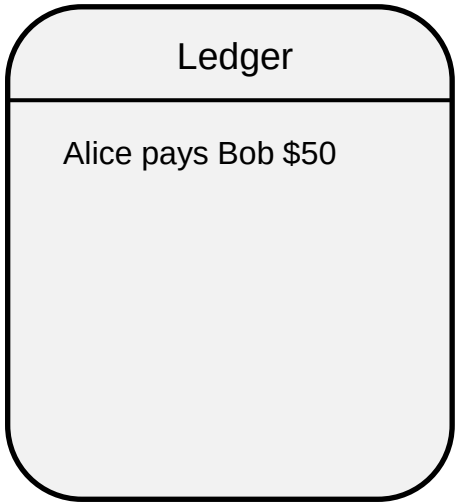


Bob

Ledger

Alice

Charlie



Bob

Ledger

Alice

Charlie

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob

Ledger

Alice

Charlie

Bob

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Ledger

Alice

Charlie

Bob

Ledger
Alice pays Bob $50
Alice pays Charlie $20
Bob pays Charlie $100
Charlie pays Alice $30

Ledger

Alice

Charlie

Bob

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Charlie pays Alice $30

…

Bitcoin from 10000ft

- Let’s propose a digital currenccy:
  e-Kuna

e-Kuna

Alice

Bob

Charlie

e-Kuna

Alice

Ledger

Bob

Charlie

e-Kuna

Alice

Ledger

Alice pays Bob $50

Bob

Charlie

e-Kuna

Alice

Charlie

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob

e-Kuna

Alice

Charlie

Ledger
Alice pays Bob $50
Alice pays Charlie $20
Bob pays Charlie $100

Bob

e-Kuna

Where do we store the ledger?

Alice

Charlie

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Bob

e-Kuna

Is this secure?

Alice

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Bob

Charlie

e-Kuna

Is this secure?

Anonymous

Alice

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Bob

Charlie

e-Kuna

Is this secure?

Anonymous

Alice

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Bob pays Anonymous $200

Bob

Charlie

e-Kuna

Is this secure?

Anonymous

Alice

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Bob pays Anonymous $200

Alice pays Anonymous $50

Bob

Charlie

e-Kuna

How to solve the hacking issue?

Alice

Charlie

Ledger

Alice pays Bob $50

Alice pays Charlie $20

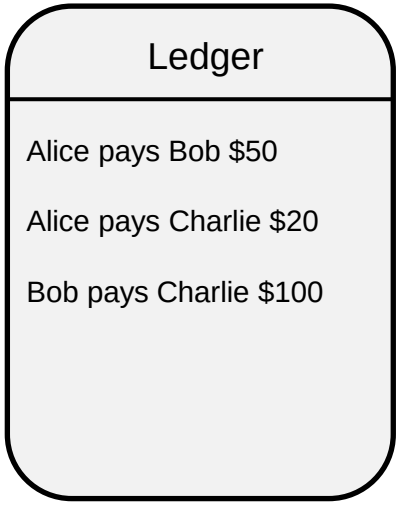
Bob pays Charlie $100

Bob

e-Kuna

Everyone stores a copy of the ledger

Alice



Bob

Charlie

e-Kuna

Everyone stores a copy of the ledger

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Alice

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Bob

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Charlie

e-Kuna

Everyone stores a copy of the ledger

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Alice

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Bob

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Charlie

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Problem 1 with e-Kuna

The ledger can be quite big

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Alice

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

200GB

Bob

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Charlie

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Problem 1 with e-Kuna

The ledger can be quite big

200GB

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Alice

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

200GB

Bob

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

200GB

Charlie

200GB

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Problem 2 with e-Kuna

Who adds the transactions?

Alice

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Bob

Charlie

Problem 2 with e-Kuna

Who adds the transactions?

Alice

Charlie

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Alice pays Bob $20000

Bob

Problem 3 with e-Kuna

Consistent historic data

Ledger
Alice pays Bob $50
Alice pays Charlie $20
Bob pays Charlie $100
Charlie pays Alice $40
. . .

Alice

Bob

Charlie

Problem 3 with e-Kuna

Consistent historic data

Ledger 1
Alice pays Bob $50
Alice pays Charlie $20
Bob pays Charlie $100
Charlie pays Alice $40
. . .

Ledger 2
Bob pays Charlie $250

Alice

Bob

Charlie

Problem 3 with e-Kuna

Consistent historic data

Ledger 1
Alice pays Bob $50
Alice pays Charlie $20
Bob pays Charlie $100
Charlie pays Alice $40
. . .

Ledger 2
Bob pays Charlie $250
Bob pays Alice $120
Charlie pays Alice $80
Alice pays Bob $20
Alice pays Charlie $10

Alice

Bob

Charlie

Problem 3 with e-Kuna

Consistent historic data

Ledger 1	Ledger 2	Ledger 3
Alice pays Bob $50	Bob pays Charlie $250	Alice pays Bob $20
Alice pays Charlie $20	Bob pays Alice $120	Alice pays Charlie $10
Bob pays Charlie $100	Charlie pays Alice $80	Bob pays Charlie $100
Charlie pays Alice $40	Alice pays Bob $20	Charlie pays Alice $40
. . .	Alice pays Charlie $10	

Alice

Bob

Charlie

Problem 3 with e-Kuna

Consistent historic data

Ledger 1	Ledger 2	Ledger 3
Alice pays Bob $50	Bob pays Charlie $250	Alice pays Bob $20
Alice pays Charlie $20	Bob pays Alice $120	Alice pays Charlie $10
Bob pays Charlie $100	Charlie pays Alice $80	Bob pays Charlie $100
Charlie pays Alice $40	Alice pays Bob $20	Charlie pays Alice $40
. . .	Alice pays Charlie $10	

Alice

Bob

Charlie

Problem 3 with e-Kuna

Consistent historic data

Ledger 1	Ledger 2	Ledger 3
Alice pays Bob $50	Bob pays Charlie $250	Alice pays Bob $20
Alice pays Charlie $20	Bob pays Alice $20	Alice pays Charlie $10
Bob pays Charlie $100	Charlie pays Alice $80	Bob pays Charlie $100
Charlie pays Alice $40	Alice pays Bob $20	Charlie pays Alice $40
. . .	Alice pays Charlie $10	

Alice

Bob

Charlie

Problem 4 with e-Kuna

What happens when Bob leaves?

Ledger 1
Alice pays Bob $50
Alice pays Charlie $20
Bob pays Charlie $100
Charlie pays Alice $40
. . .

Ledger 2
Bob pays Charlie $250
Bob pays Alice $120
Charlie pays Alice $80
Alice pays Bob $20
Alice pays Charlie $10

Ledger 3
Alice pays Bob $20
Alice pays Charlie $10
Bob pays Charlie $100
Charlie pays Alice $40

Alice

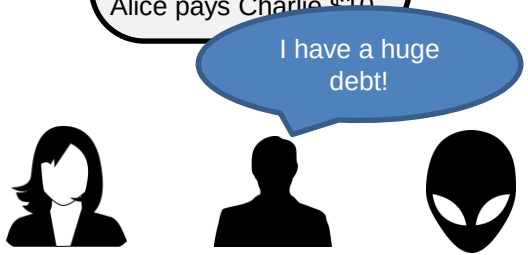
Bob

Charlie

Problem 4 with e-Kuna

What happens when Bob leaves?

Ledger 1	Ledger 2	Ledger 3
Alice pays Bob $50	Bob pays Charlie $250	Alice pays Bob $20
Alice pays Charlie $20	Bob pays Alice $120	Alice pays Charlie $10
Bob pays Charlie $100	Charlie pays Alice $80	Bob pays Charlie $100
Charlie pays Alice $40	Alice pays Bob $20	Charlie pays Alice $40
. . .	Alice pays Charlie $10	



Problem 4 with e-Kuna

What happens when Bob leaves?

Ledger 1	Ledger 2	Ledger 3
Alice pays Bob $50	Bob pays Charlie $250	Alice pays Bob $20
Alice pays Charlie $20	Bob pays Alice $120	Alice pays Charlie $10
Bob pays Charlie $100	Charlie pays Alice $80	Bob pays Charlie $100
Charlie pays Alice $40	Alice pays Bob $20	[illegible] pays Alice $40
. . .	Alice pays Charlie $10	

Alice Bob Charlie

Problem 4 with e-Kuna

What happens when Bob leaves?

Ledger 1
Alice pays Bob $50
Alice pays Charlie $20
Bob pays Charlie $100
Charlie pays Alice $40
. . .

Ledger 2
Bob pays Charlie $250
Bob pays Alice $120
Charlie pays Alice $80
Alice pays Bob $20
Alice pays Charlie $10

Ledger 3
Alice pays Bob $20
Alice pays Charlie $10
Bob pays Charlie $100
Charlie pays Alice $40

Alice

Charlie

Problem 5 with e-Kuna

Who manages the master ledger?

Alice

Charlie

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Bob

Problem 5 with e-Kuna

Who manages the master ledger?

Alice

Charlie

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Bob

Problem 5 with e-Kuna

Who manages the master ledger?

Alice

Charlie

Ledger

Alice pays Bob $50

Alice pays Charlie $20

Bob pays Charlie $100

Bob

BitCoin

How to solve the problems of e-Kuna?

- Problem 1 – hash functions
- Problem 2 – digital signatures
- Problem 3 - blockchain
- Problem 4 – where does the money come from
- Problem 5 – decentralisation in Bitcoin