Blockchain: opportunities, challenges and use cases

Valentina Gatteschi
Politecnico di Torino - Dipartimento di Automatica e Informatica
GRAINS Group - http://grains.polito.it/
e-mail: valentina.gatteschi@polito.it
website: http://staff.polito.it/valentina.gatteschi/

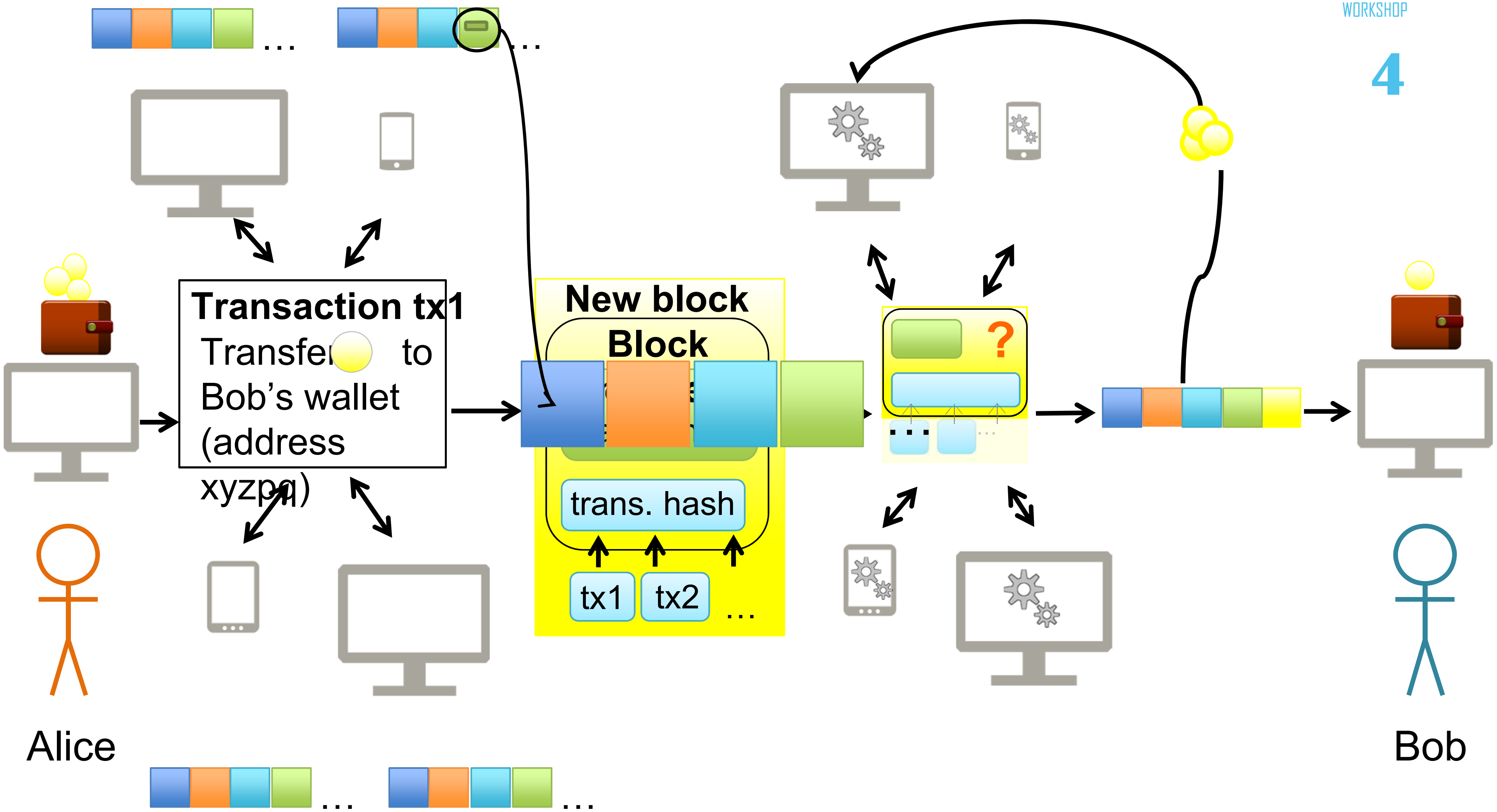
GRAINS
GRAphics and INtelligent Systems group

BLOCKCHAIN 101

DEFINITION

A blockchain is a:

- distributed ledger
- maintained by network nodes
- recording transactions (messages sent from one node to another) executed among network participants



Transaction tx1

Transfer ○ to Bob’s wallet (address xyzpq)

New block

Block

trans. hash

tx1 tx2 …

Alice

Bob

But it’s not only for money…

“What if we store on the blockchain other kind of information?”

VITALIK BUTERIN

CREATOR OF ETHEREUM

“Why don’t we store pieces of code?”

SMART CONTRACTS

- Small programs stored on the blockchain and programmed to autonomously behave in a given manner, if some conditions are met

<code>

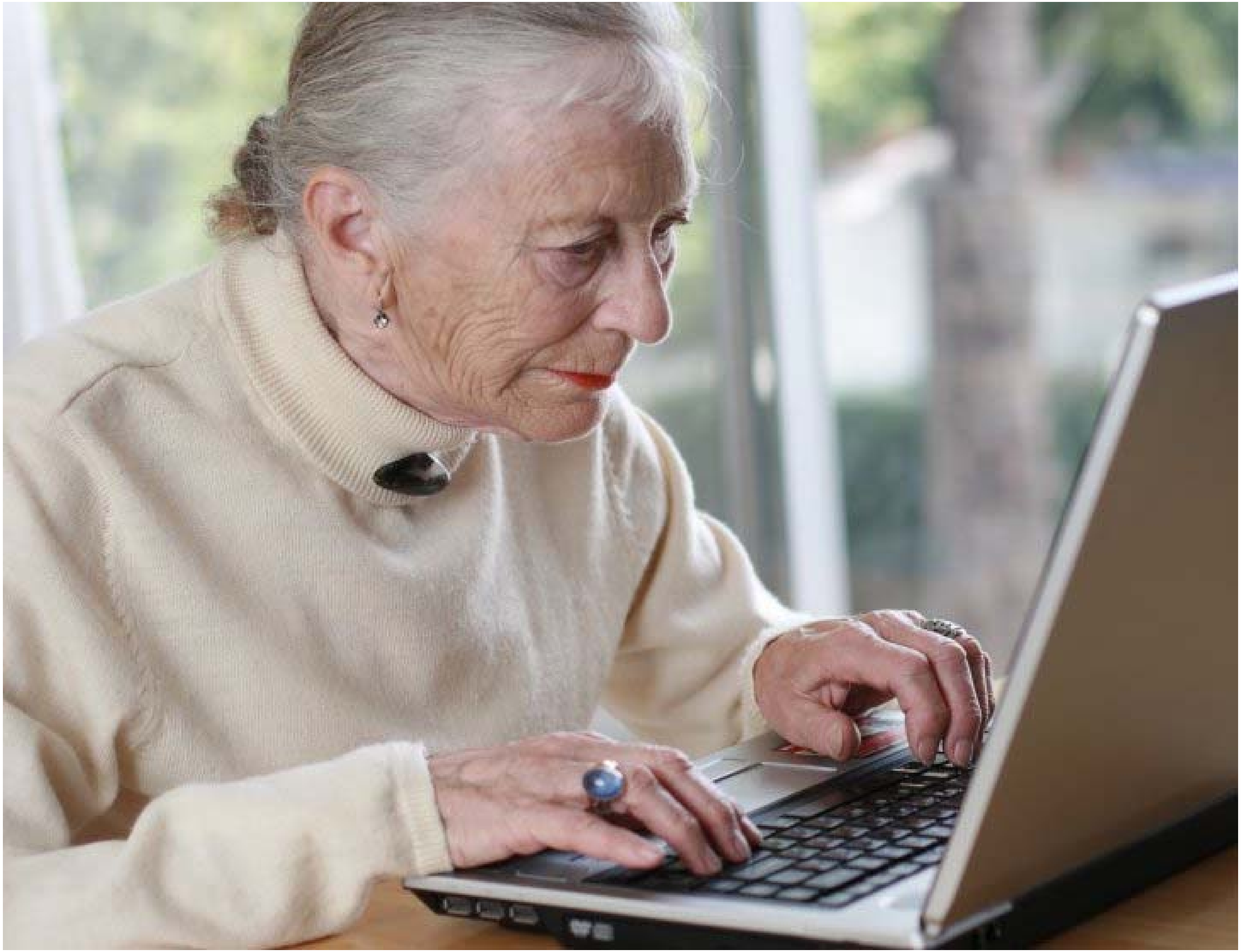
“When I die, give everything I have to my grandchild
only if he graduates”

</code>

A PRACTICAL EXAMPLE

Alice

Images courtesy of Freepik, Superawesomevectors, the Noun Project, Know Your Meme

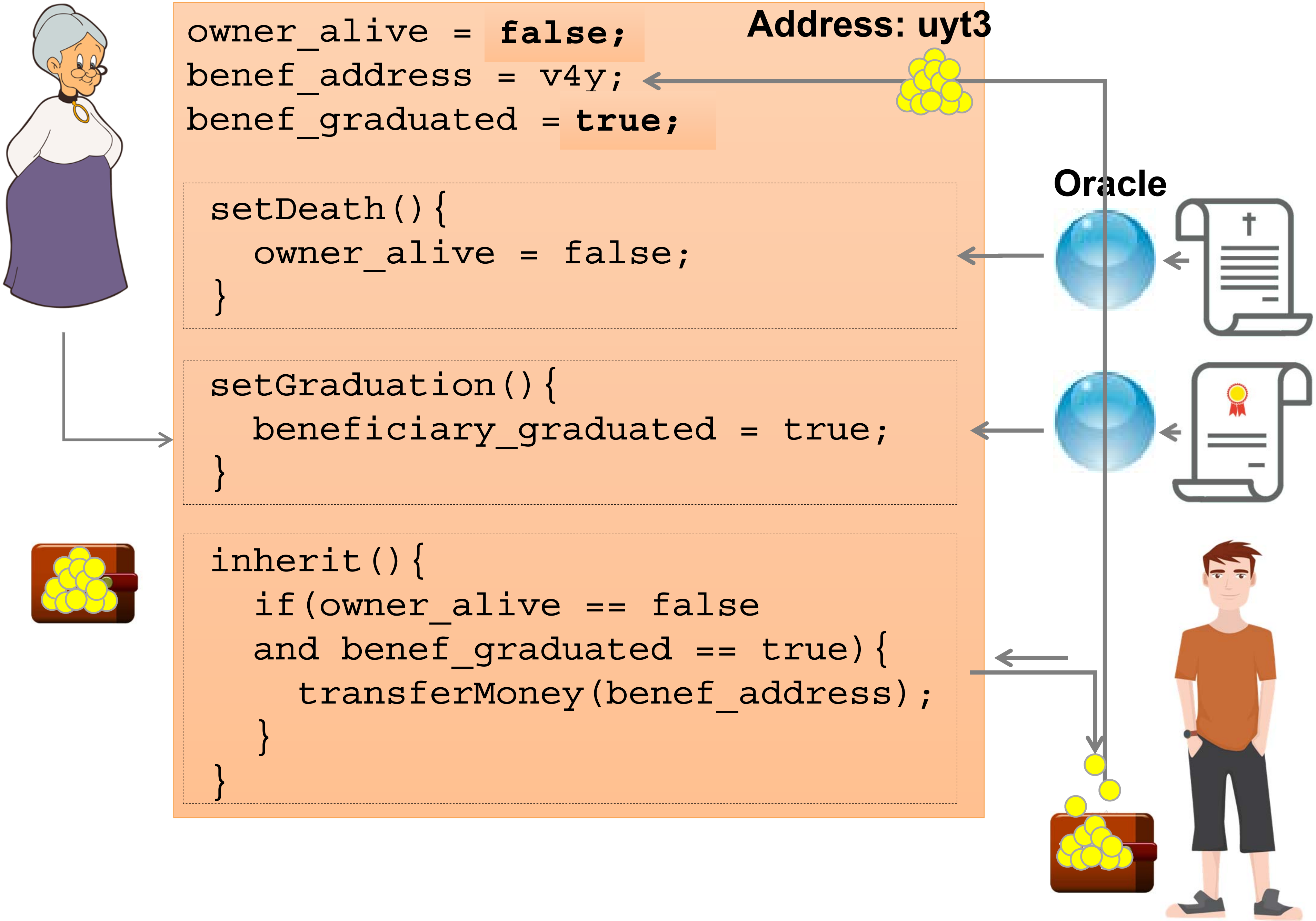


A PRACTICAL EXAMPLE

Alice

Bob

Images courtesy of Freepik, Superawesomevectors, the Noun Project, Know Your Meme



Smart contract

Address: uyt3

```
owner_alive = false;
benef_address = v4y;
benef_graduated = true;

setDeath(){
   owner_alive = false;
}

setGraduation(){
   beneficiary_graduated = true;
}

inherit(){
   if(owner_alive == false
   and benef_graduated == true){
      transferMoney(benef_address);
   }
}
```

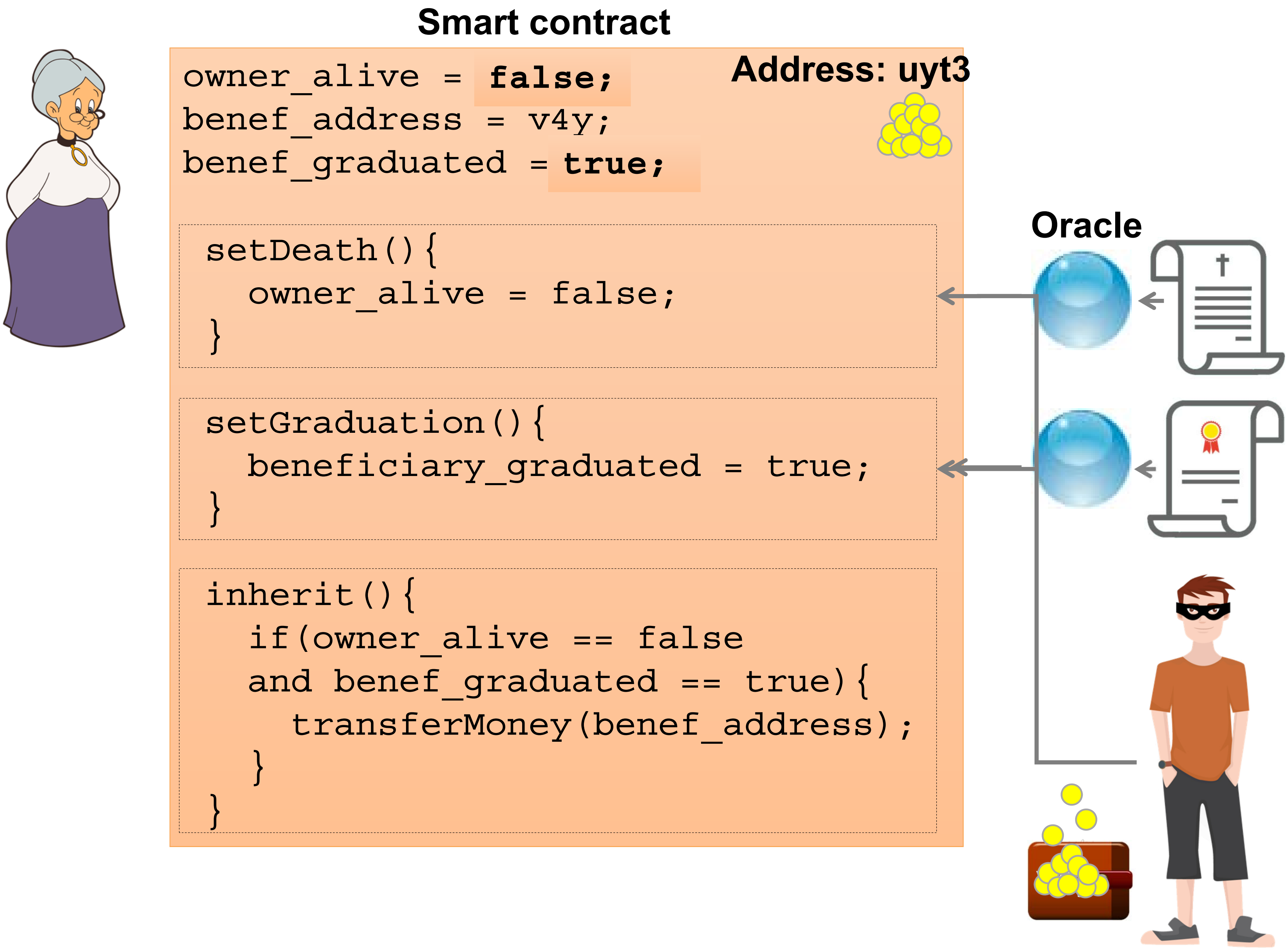
BUT…

- Technical issues

- Other issues

BUT…

- Technical issues
  - Code could contain bugs!



Smart contract

Address: uyt3

```
owner_alive = false;
benef_address = v4y;
benef_graduated = true;

setDeath(){
   owner_alive = false;
}

setGraduation(){
   beneficiary_graduated = true;
}

inherit(){
   if(owner_alive == false
   and benef_graduated == true){
      transferMoney(benef_address);
   }
}
```

Oracle

BUT…

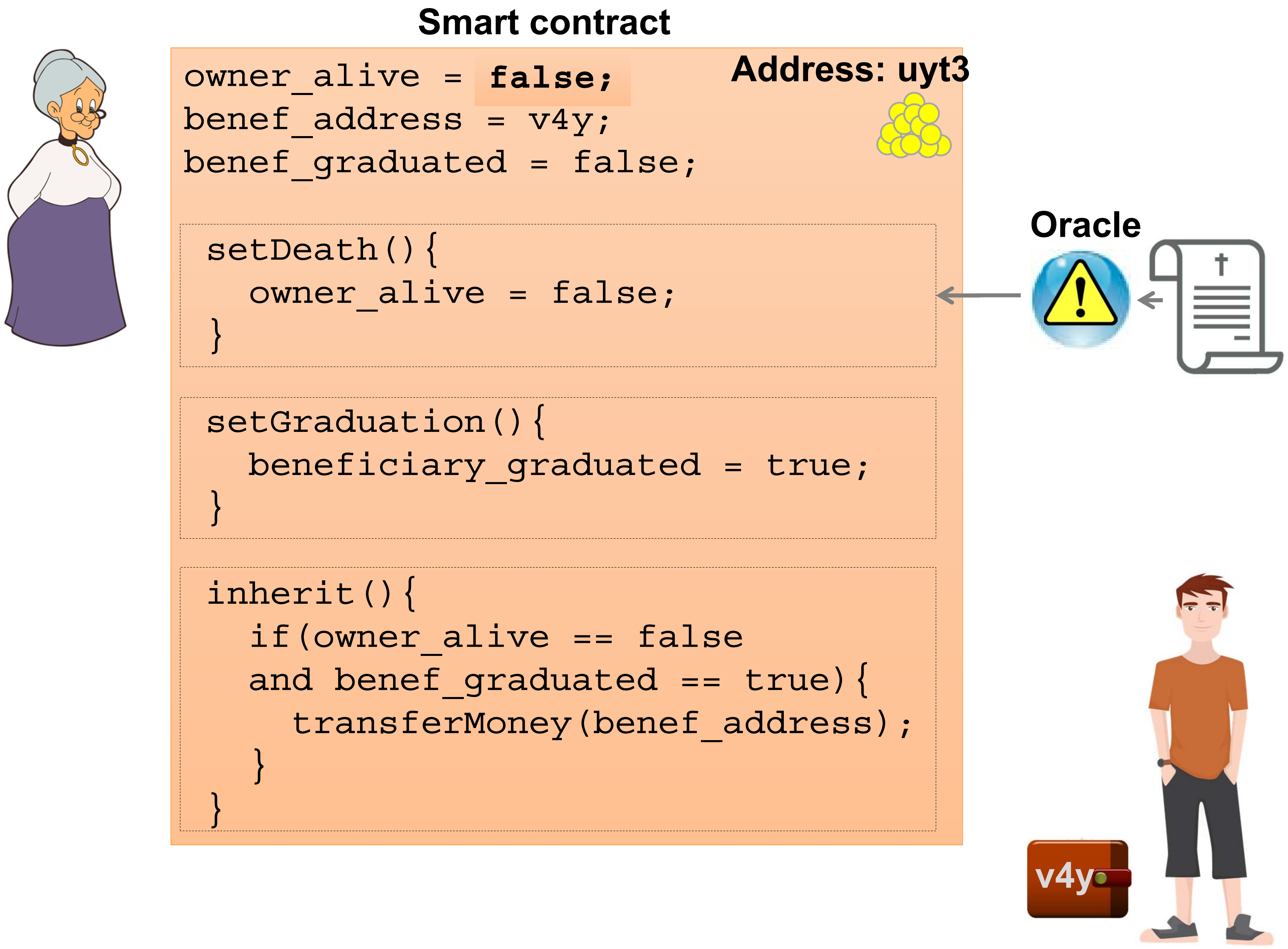
- Technical issues
  - Code could contain bugs!

SOLUTION

- Thoroughly write code
- Rely on White Hat Hackers
  - Bounty programs
  - Hacken.io
  - …

BUT…

- Technical issues
  - Code could contain bugs!
  - Oracles could inject wrong information



Smart contract

Address: uyt3

```
owner_alive = false;
benef_address = v4y;
benef_graduated = false;

 setDeath(){
   owner_alive = false;
 }

 setGraduation(){
   beneficiary_graduated = true;
 }

 inherit(){
   if(owner_alive == false
   and benef_graduated == true){
     transferMoney(benef_address);
   }
 }
```

Oracle

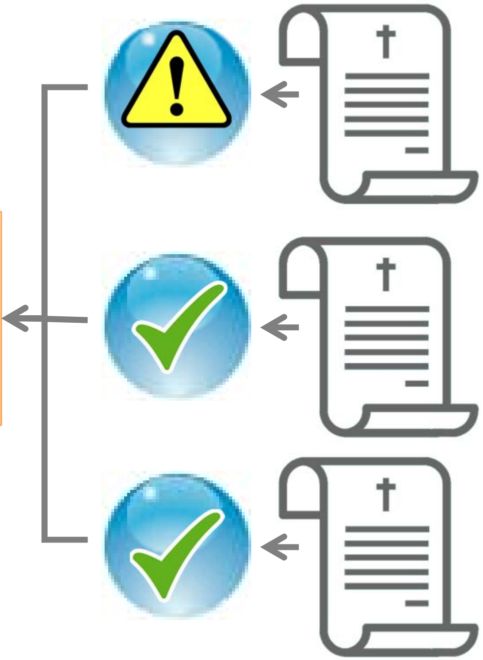
BUT...

- Technical issues
  - Code could contain bugs!
  - Oracles could inject wrong information

SOLUTION

- Rely on more than one oracle

```
setDeath(){
   owner_alive = false;
}
```



BUT...

- Technical issues
  - Code could contain bugs!
  - Oracles could inject wrong information

- Other issues
  - What if Ethereum is no longer used/supported?

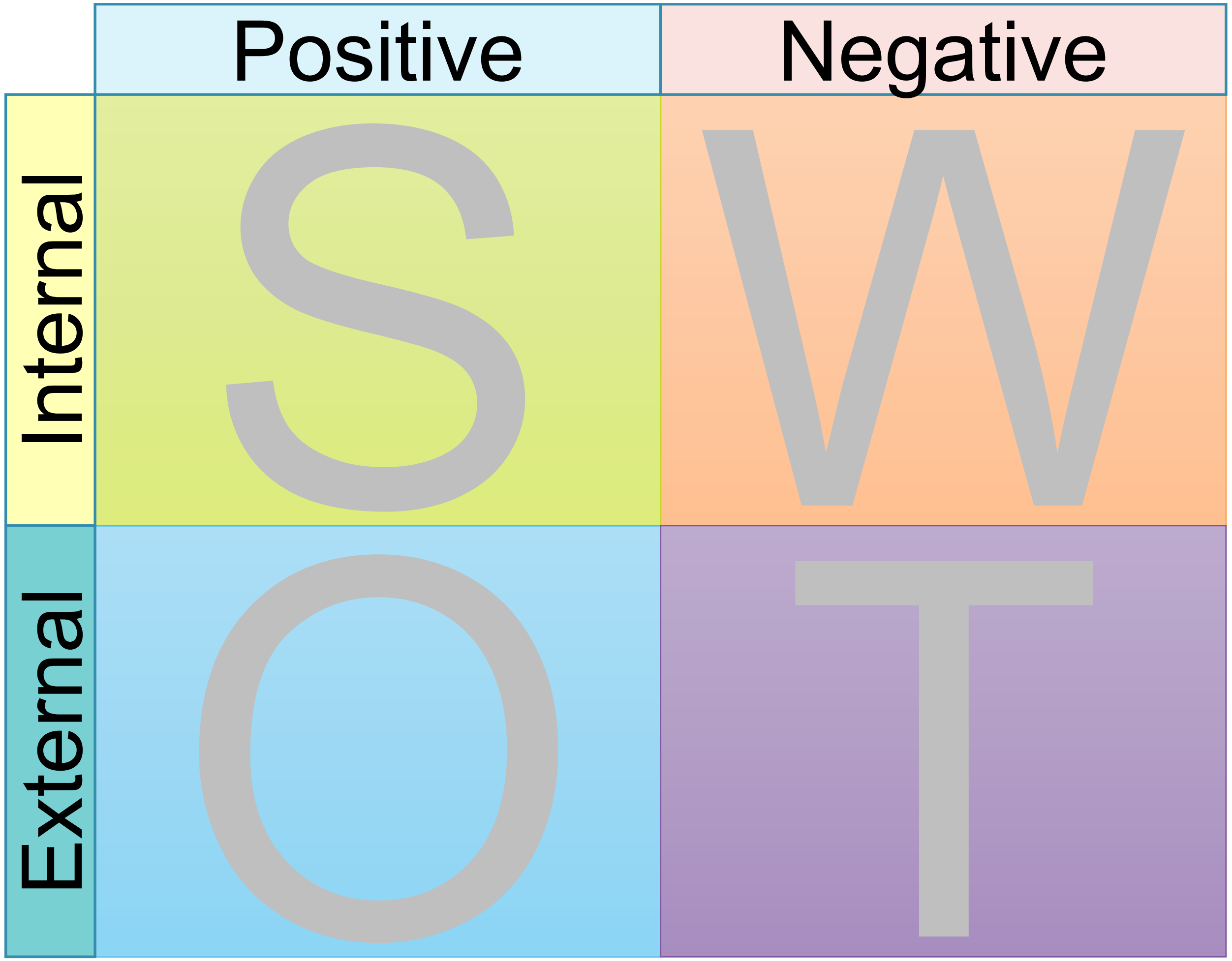
BUT…

- Technical issues
  - Code could contain bugs!
  - Oracles could inject wrong information

- Other issues
  - What if Ethereum is no longer used/supported?
  - Volatility of cryptocurrencies

Is it worth it?

SWOT – Adoption of blockchain



	Positive	Negative
Internal	S	W
External	O	T

V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, V. Santamaría, "Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?" *Future Internet* 2018, 10, 20

STRENGTHS

- Fast and low-cost money transfers
- No need for intermediaries
- Automation (smart contracts)
- Accessible worldwide
- Transparency
- Platform for data analytics
- No data loss/modification/falsification
- Non-repudiation

WEAKNESSES

- Scalability
- Low performance
- Energy consumption
- Reduced users’ privacy
- Autonomous code is “candy for hackers”
- Need to rely to external oracles
- No intermediary to contact in case of loss of users’ credentials
- Volatility of cryptocurrencies
- Still in an early stage (no “winning” blockchain)
- Same results achieved with well-mastered technologies

OPPORTUNITIES

- Competitive advantage
- Possibility to address new markets (e.g., supporting car and house sharing, disk storage rental, etc.)
- Availability of a huge amount of heterogeneous data (by different actors)

THREATS

- Could be perceived as unsecure/unreliable
- Low adoption from external actors
- Governments could consider it “dangerous”
- Medium-long term investment
- Customers would still consider personal interaction important

Use cases

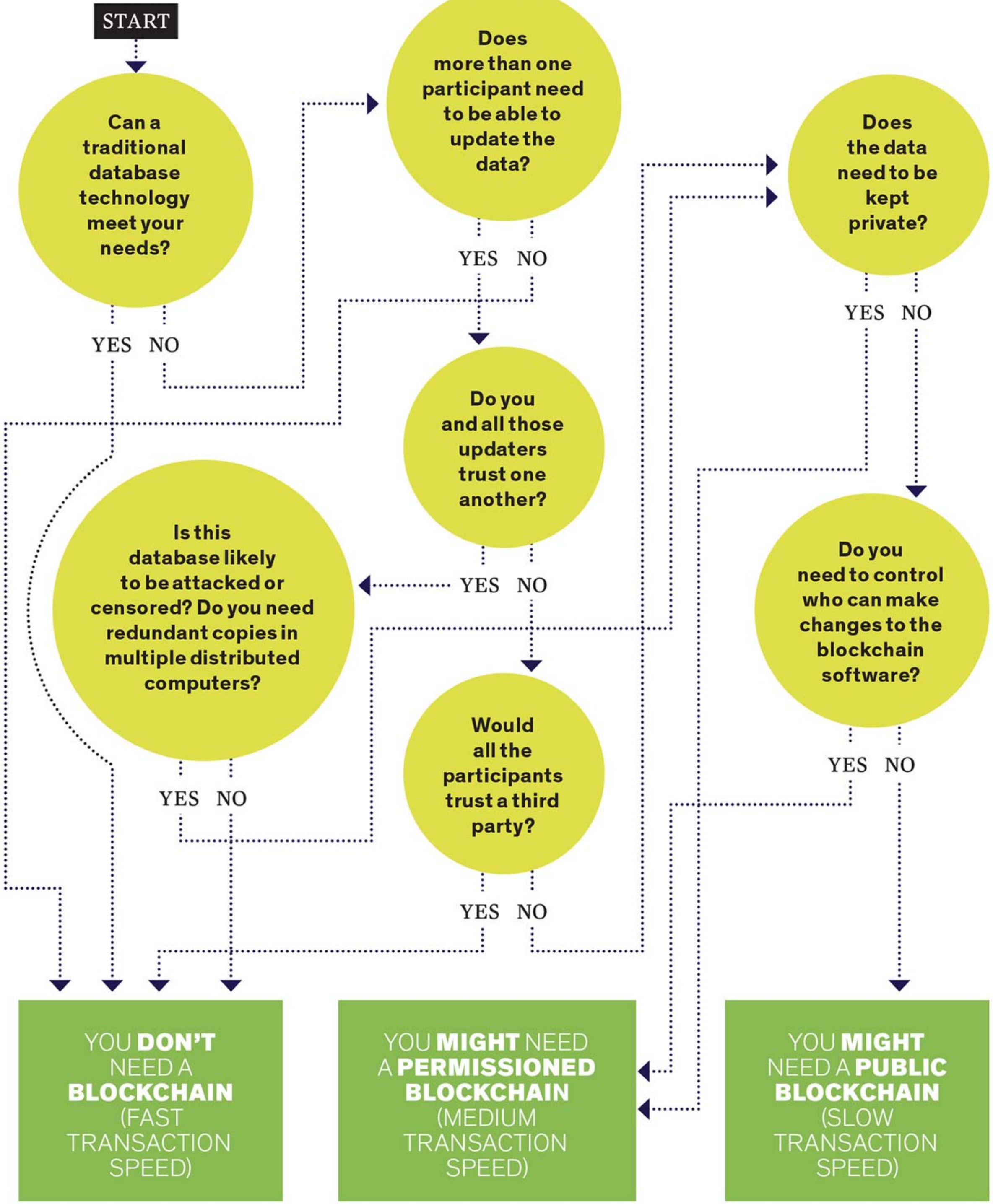
USE CASES

- Personal data management
  - proof of identity, KYC, etc.
- Notary services
  - store public records (marriages, etc.), intellectual property rights protection, etc.
- Finance
  - money transfers, decentralized exchanges, online lotteries, smart contract-based pension funds, etc.
- Industry/commerce
  - supply chain, prevent counterfeit items, management of interaction between seller and buyer, support of demand-driven economy through smart contracts

USE CASES

- Insurance
  - automatic claim processing (smart contracts + sensors), KYC, reducing frauds, pay-per-use insurance, peer-to-peer insurances, etc.
- Government, healthcare, education
  - record citizens' votes, autonomous governance systems, store patient's medical data, record competencies, etc.
- Software, Internet, IoT
  - store system logs, domain names, cloud storage, authentication of IoT devices, automatic interaction of intelligent appliances with real world, smart grid, etc.
- …

Do you need a blockchain?



START

Can a traditional database technology meet your needs?

YES NO

Does more than one participant need to be able to update the data?

YES NO

Do you and all those updaters trust one another?

YES NO

Would all the participants trust a third party?

YES NO

Is this database likely to be attacked or censored? Do you need redundant copies in multiple distributed computers?

YES NO

Does the data need to be kept private?

YES NO

Do you need to control who can make changes to the blockchain software?

YES NO

YOU **DON'T** NEED A **BLOCKCHAIN** (FAST TRANSACTION SPEED)

YOU **MIGHT** NEED A **PERMISSIONED BLOCKCHAIN** (MEDIUM TRANSACTION SPEED)

YOU **MIGHT** NEED A **PUBLIC BLOCKCHAIN** (SLOW TRANSACTION SPEED)

M. E. Peck, "Blockchain world - Do you need a blockchain? This chart will tell you if the technology can solve your problem," in *IEEE Spectrum*, vol. 54, no. 10, pp. 38-60, October

Thank you!

Valentina Gatteschi
Politecnico di Torino - Dipartimento di Automatica e Informatica
GRAINS Group - http://grains.polito.it/
e-mail: valentina.gatteschi@polito.it
website: http://staff.polito.it/valentina.gatteschi/

V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, V. Santamaría, "To Blockchain or Not to Blockchain: That Is the Question" *IT PROFESSIONAL* 2018, 20, 2.

F. Lamberti, V. Gatteschi,, C. Demartini, M. Pelissier, A. Gómez, V. Santamaría, "On-demand Blockchain-based car insurance using smart contracts and sensors" *IEEE CONSUMER ELECTRONICS MAGAZINE* 2018, (In press).

V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, V. Santamaría, "Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?" *Future Internet* 2018, *10*, 20.