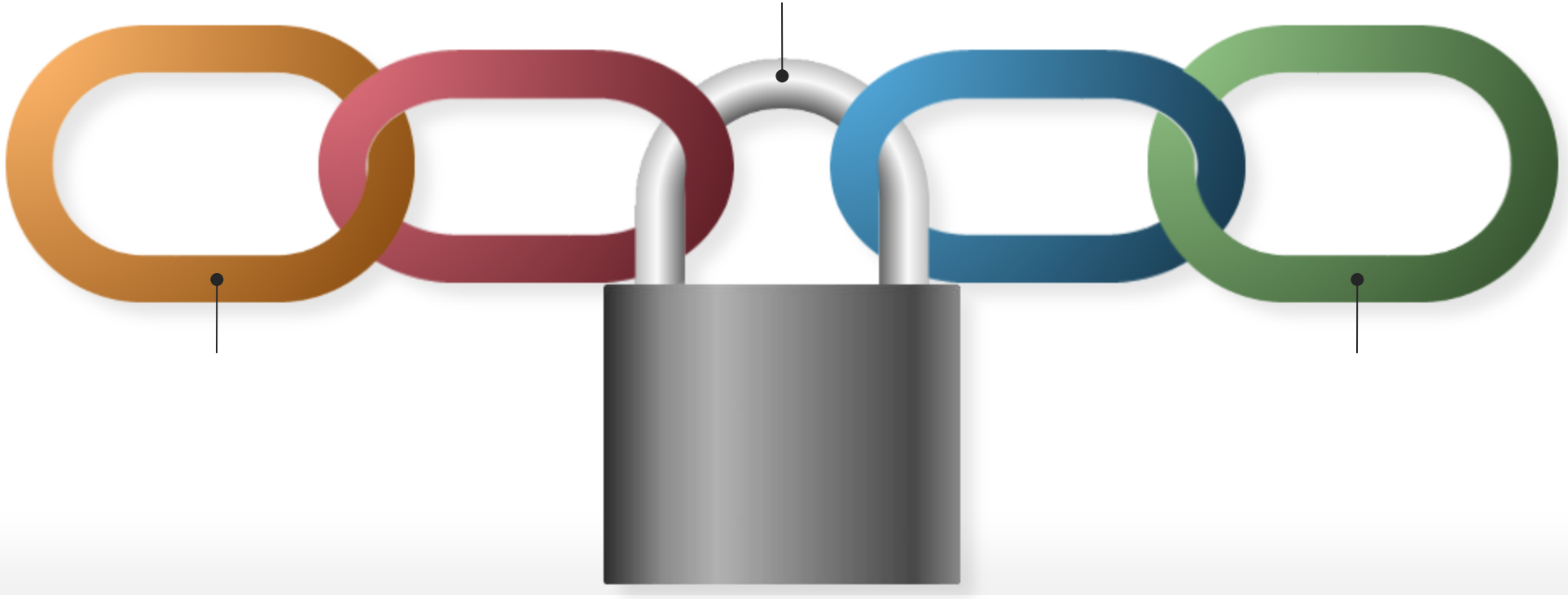
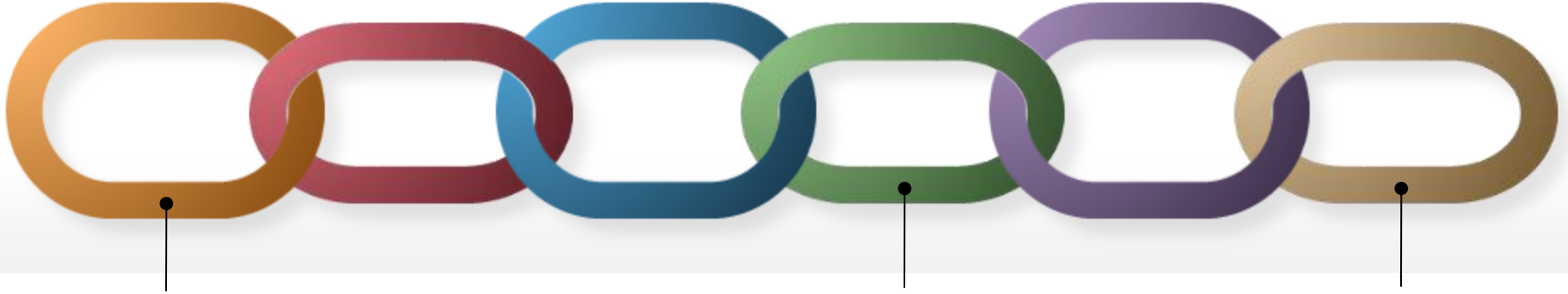


Cryptography for Blockchain Technology

Ivan Visconti

Università di Salerno (DIEM)



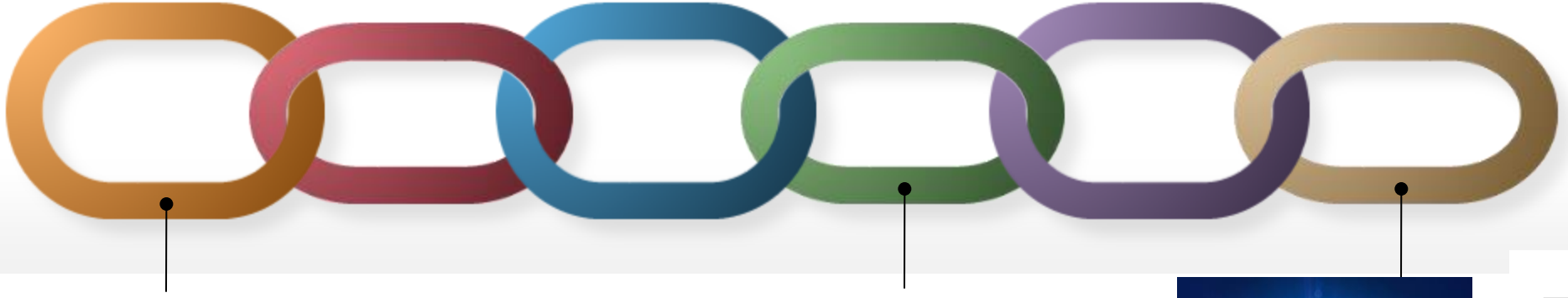
Prof. of Computer Science (DIEM, Univ. of Salerno)
contact: visconti@unisa.it

Main Research topics:

Cryptography and Blockchain Technology

Coordinator of CifrisChain

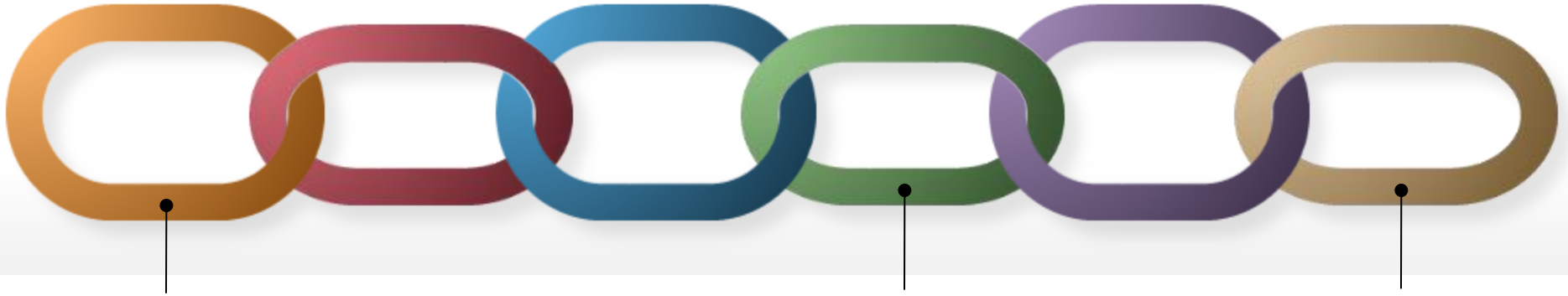
cifrischain@decifris.it



Why am I interested in blockchains?

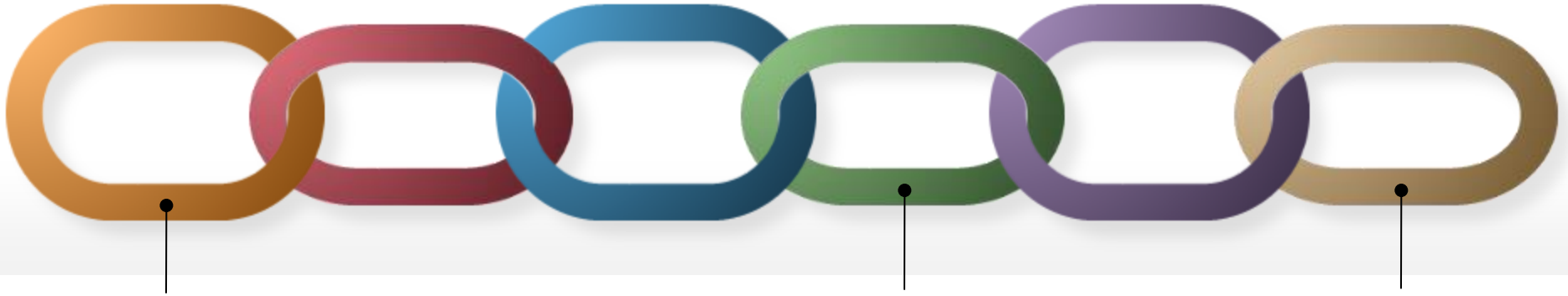
PRIVILEDGE

- Scientific coordinator for UNISA of the H2020 project **PRIViLEDGE** "*Privacy-Enhancing Cryptography in Distributed Ledgers*" (budget 4.5M EUR), a partnership with IBM Zurich, IOHK, Guardtime, U. Edinburgh....
  priviledge-project.eu
    - Lead of the workpackage "*Privacy-Enhancing Cryptography*"



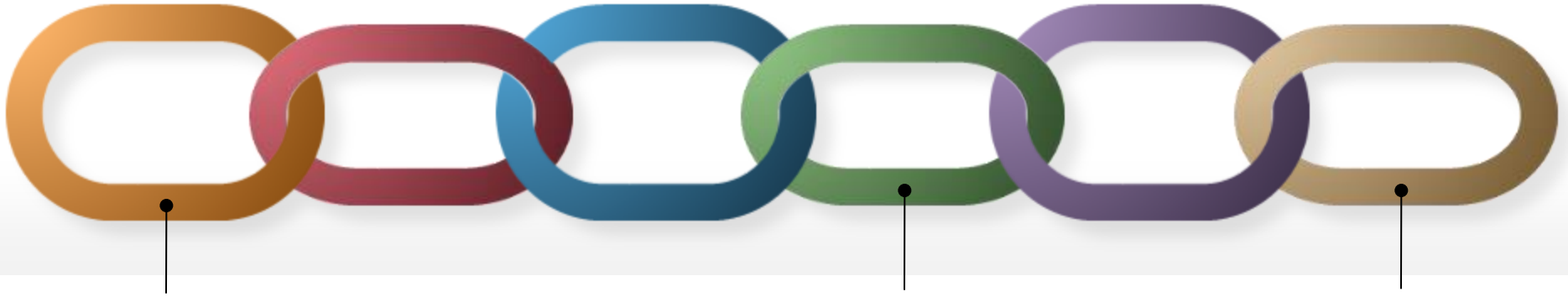
Two major goals in Cryptography

- Data Integrity
- Data Confidentiality

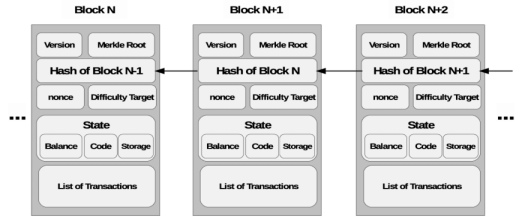


Data Integrity:
check that a message comes from Amazon

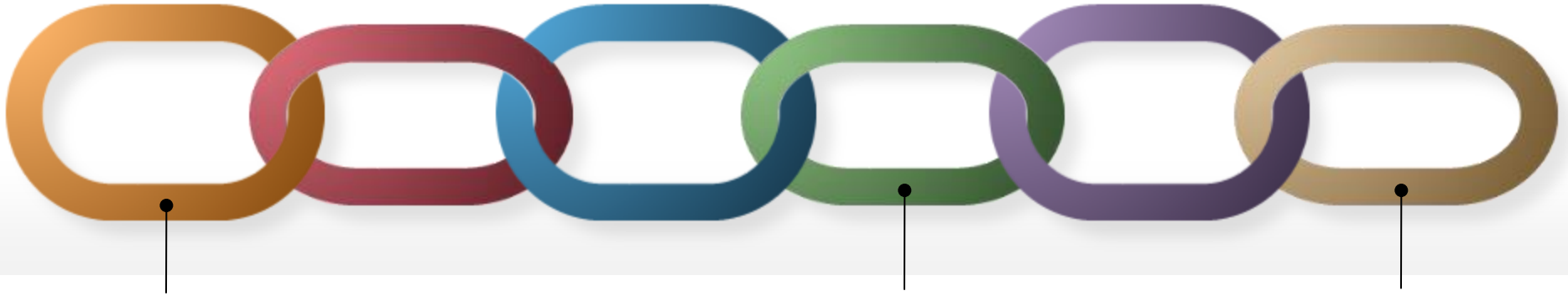
- We need computational assumptions
  (e.g., computing discrete logarithms is hard)
- We need trust assumptions (we need to trust a certification authorithy that released a digital certificate to Amazon that includes Amazon's public key for signatures)



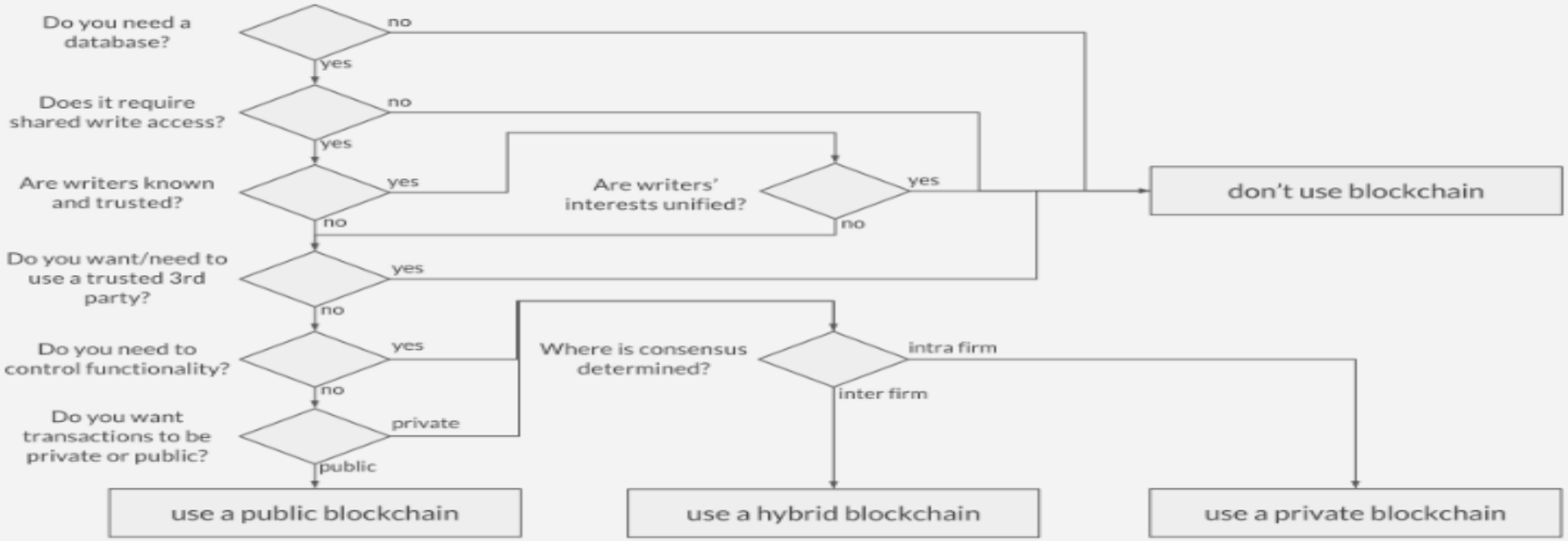
Blockchain? What is it?? Is it useful???

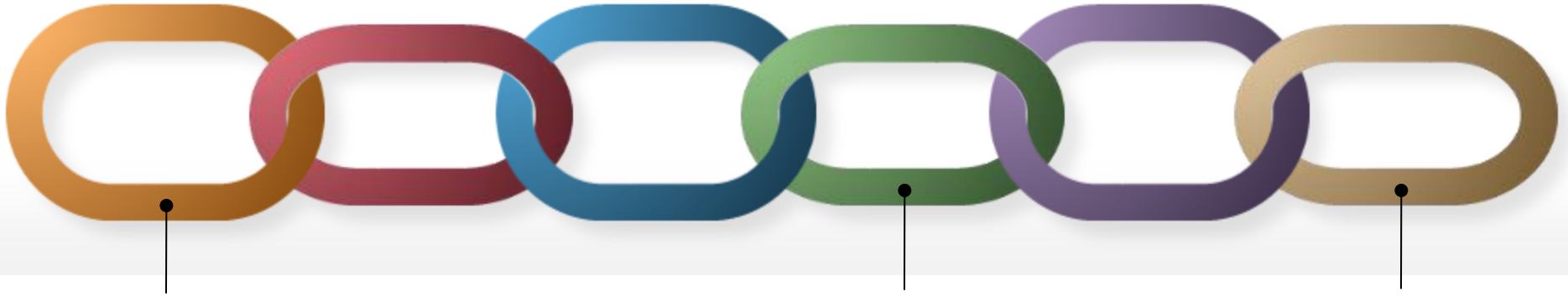


A blockchain is a sequence of blocks linked through a cryptographic hash function that can not be violated.... blablabla... it is as disruptive as the Internet, it will revolutionize our society, in Italy there is even a national strategy, there are smart contracts, ICOs, cryptocurrencies, billions of billions of...



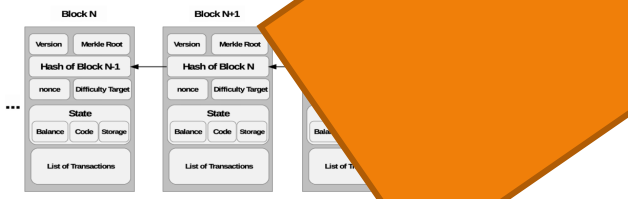
Do you even need Blockchain?

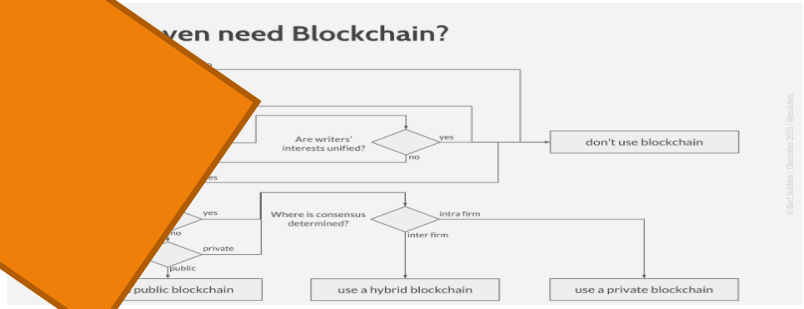


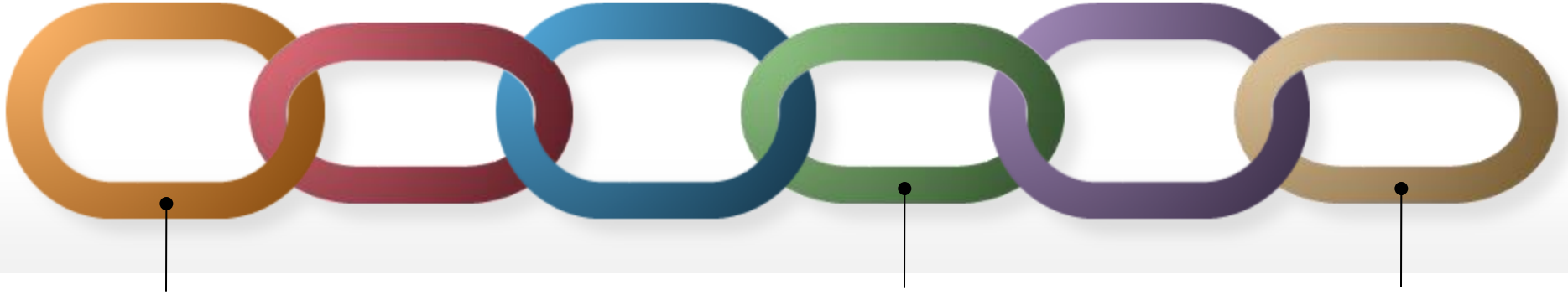


Blockchain? What is it?? Is it useful???

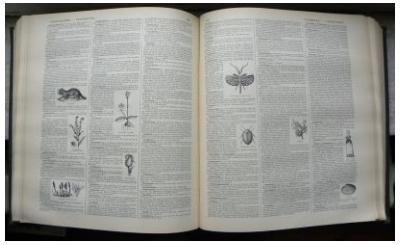
A blockchain is a sequenc… throu… hash function that can not be violated.... blabla… …will revolutionize our society, in Italy there is even nat… …t contracts, ICOs, cryptocurrencies, billions of billions …





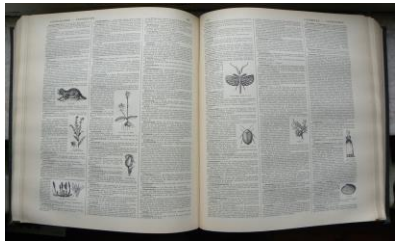


(an informal definition of blockchain)



A blockchain is a **decentralized platform** that allows the execution of **smart contracts** through the validation of transactions that updated their states

All transactions are **irreversible** (immutability)



(an informal definition of blockchain)

A blockch hat allows the execution validation of transactio

All transa y)

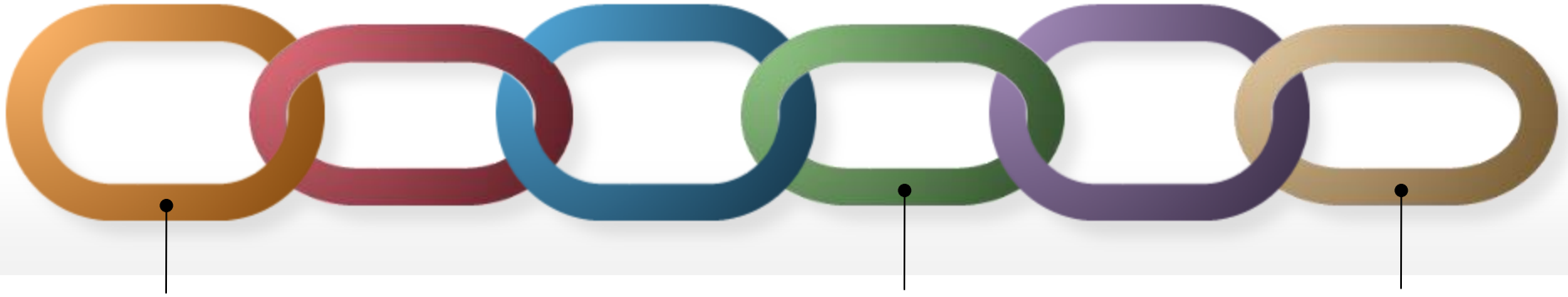
Let's be (and serious)...

to do what?

A b *decentralized* computer that *publicly* runs programs (smart contracts)

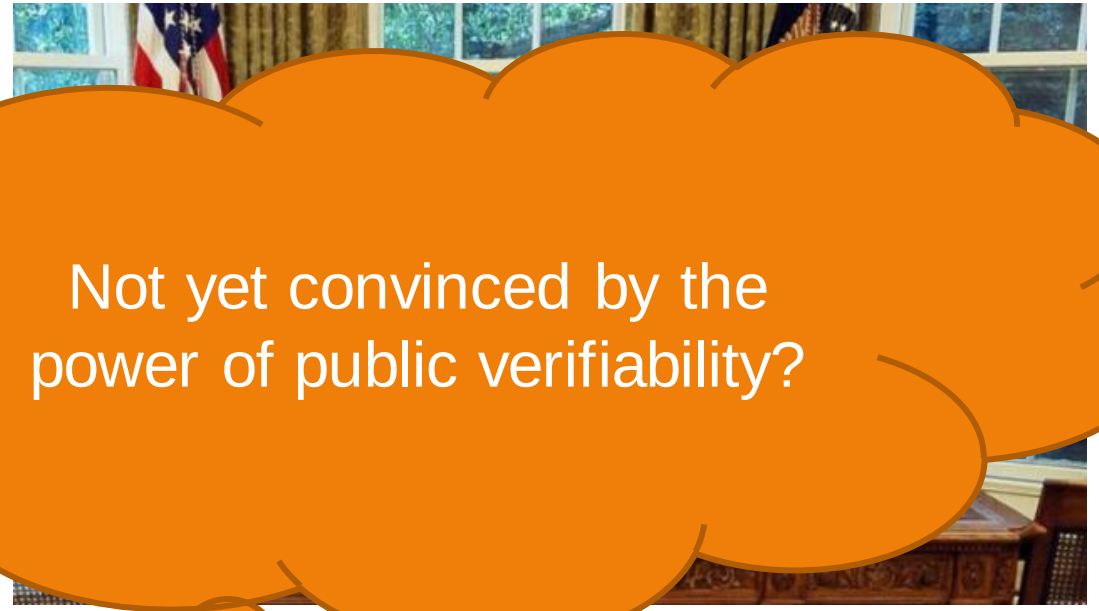
each program waits for some input (an event or a transaction) to perform some *public* task

public verifiability through immutability holds also for new computer that join the network



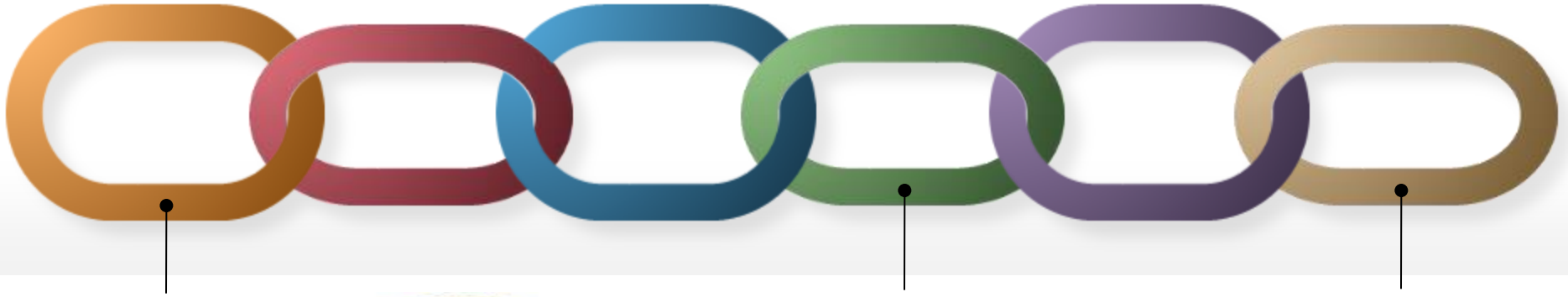
Reselience and Transparency

A decentralized computer works perfectly even in case of a large scale attack



Not yet convinced by the power of public verifiability?

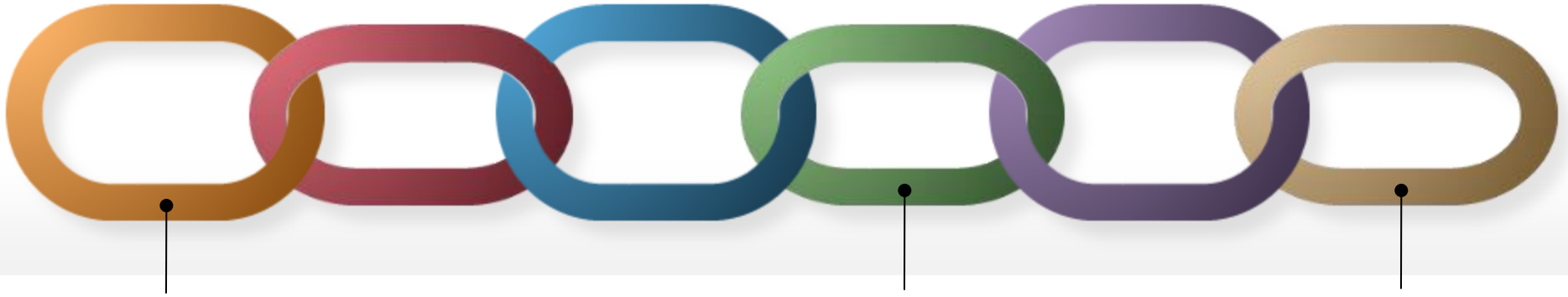
Everyone even in the future can verify the correctness of the current state of an execution of a program (and therefore of the entire decentralized computer)



Bitcoin

A blockchain running 2 programs:

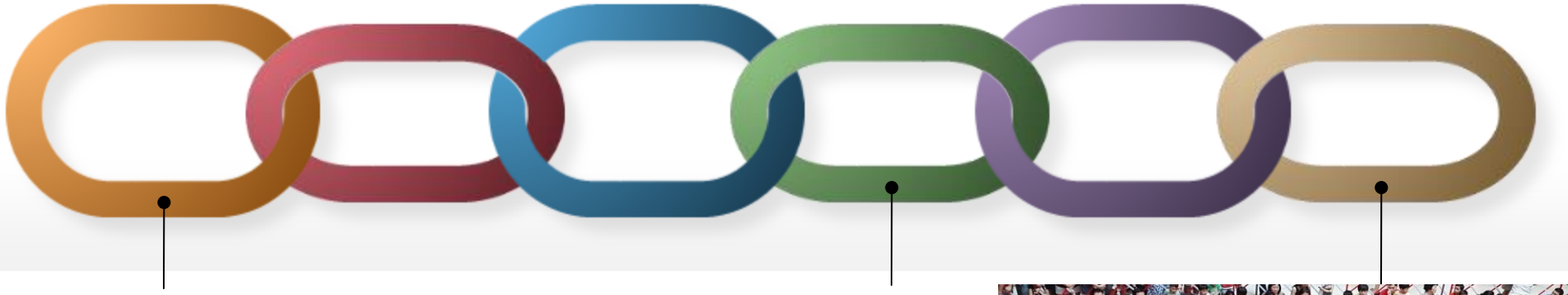
1) one to mint coins and assign them to through a lottery
2) one to transfer coins among wallets



Ethereum

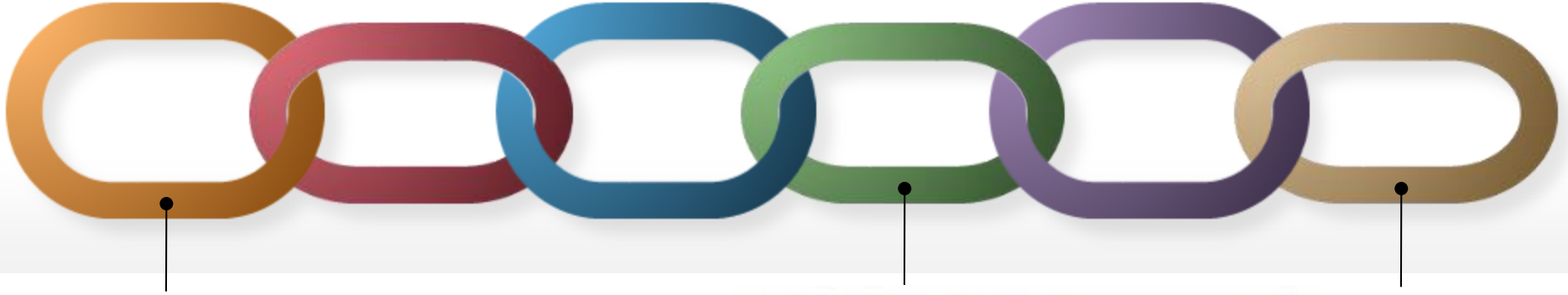
supports generic programs

Vitalik Buterin claimed that you can’t have scalability, decentralization and security at the same time…
This is the blockchain **Trilemma**.



Public verifiability is charming

Everyone can verify the current state of the execution of a smart contract starting from its creation.
Trasparency brings enthiusiasm and involvement
Wherever you need a trusted authority you might want to use a blockchain instead.



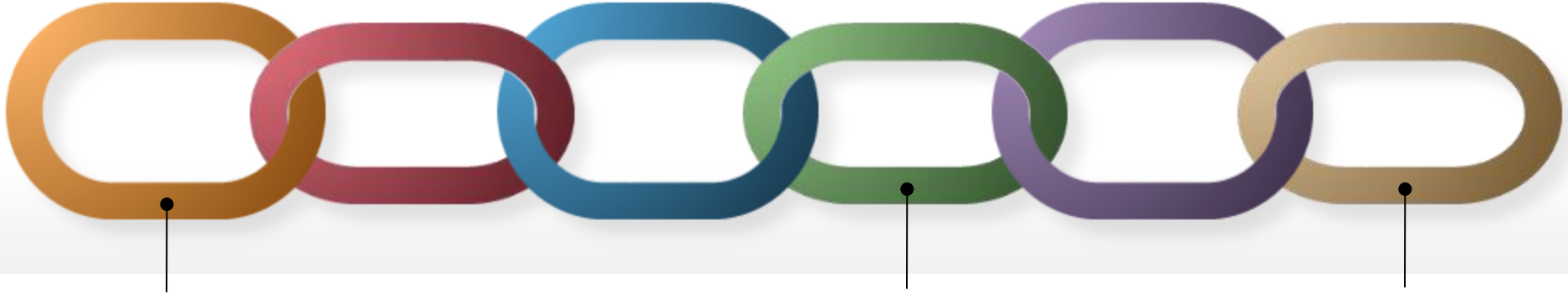
In other words....

we can consider Blockchain technology as a disruptive tool against counterfeiting of processes

it makes you worry free....

think of transferring money
to rennovate your building

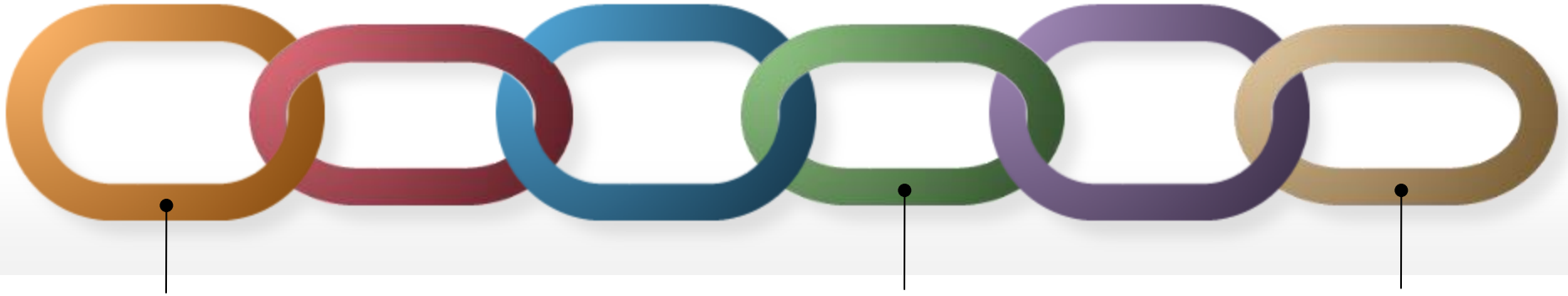
everyone living in the building can just send money to a smart contract that automatically will pay the company if that agreed total amount is reached or will return money back if a deadline expires



Let's

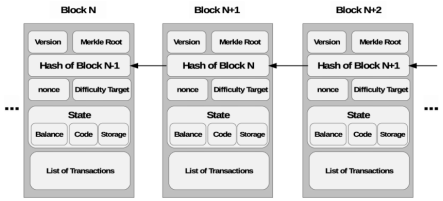
why is it called blockchain?

A blockchain is a *decentralized* computer that *publicly* runs programs (smart contracts)



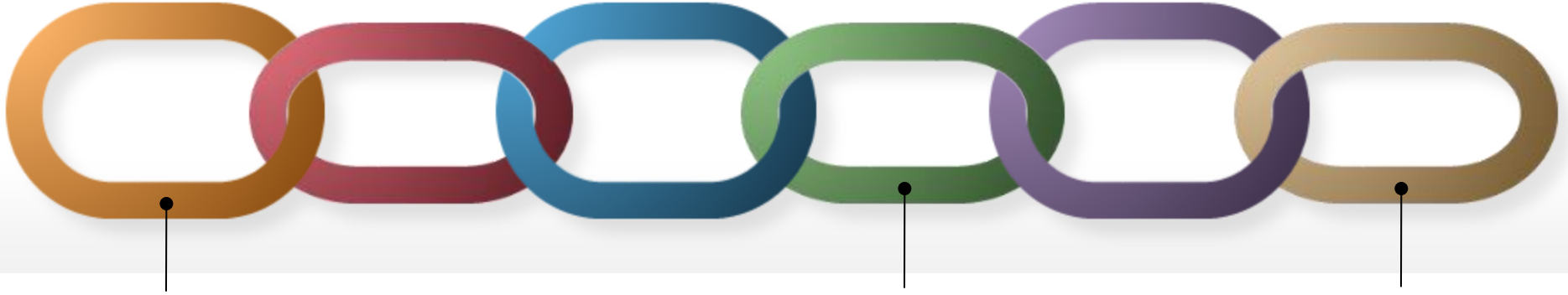
the truth is…

a chain of blocks is the tool used by Satoshi Nakamoto to design Bitcoin, the first blockchain/cryptocurrency

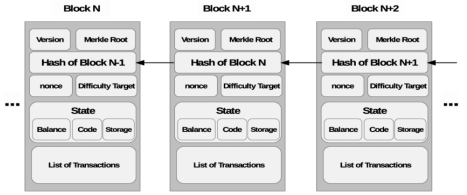


block j+1 includes a cryptographic hash of block j
$B_{j+1} = (h, B_j, \text{Transactions})$ where $h = SHA256(B_j)$

if you change B_j then B_{j+1} must be changed too

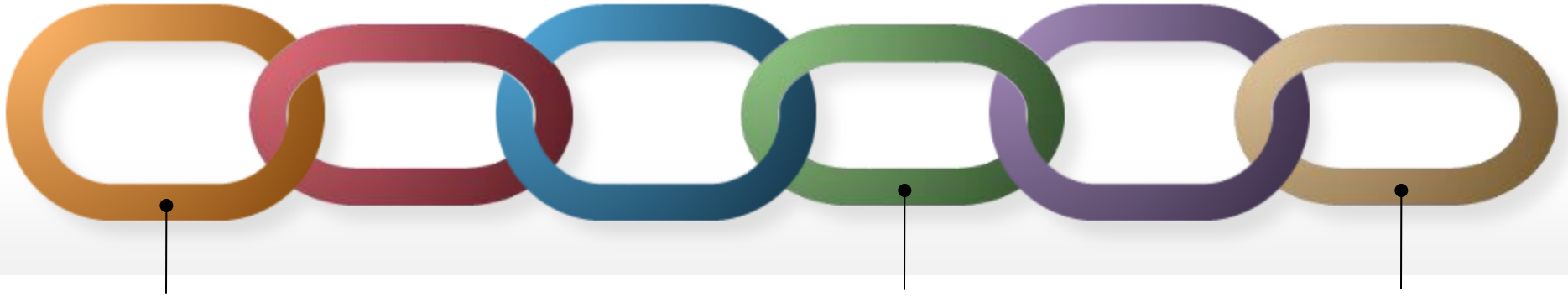


Is it easy to design a blockchain?



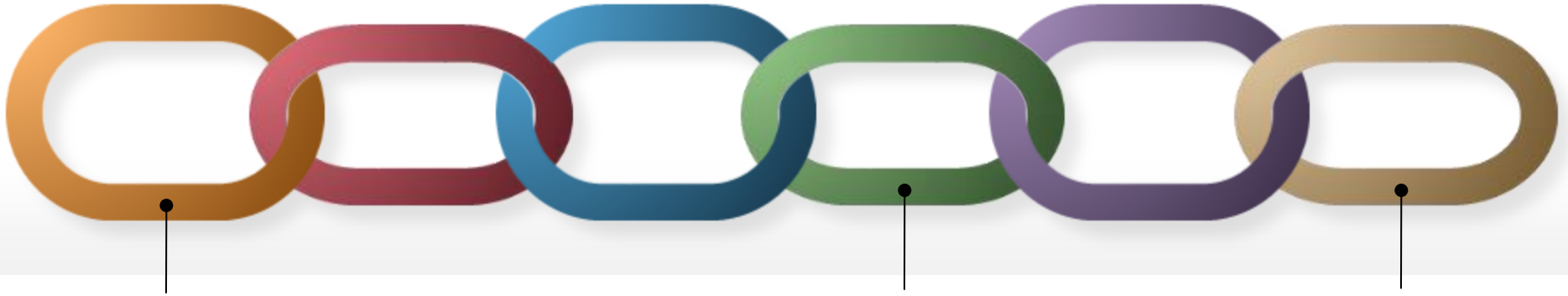
The chain of blocks (or any other technique) must uniquely identify the sequence of instructions executed by the decentralized computer

Major problem: what is the next instruction to execute (out of many candidates proposed by users through transactions)?



a new block might reach only some nodes of the network

therefore nodes might have different views of what to do next



Consensus

Consensus

Is there a honest majority?

Yes…. then there is a fast way to reach a valid agreement

No…. then there is no hope to reach a valid agreement

more or less the above results were achieved already in the 80s... assuming «one person ➔ one vote»

If players are anonymous then Consensus is impossible

Some basic cloning techniques (known as Sybil Attacks) allow the adversary to easily reach a dishonest majority

This is a limitation of the «one person ➔ one vote» approach

The breakthrough of Nakamoto

from «one person ➔ one vote»

The breakthrough of Nakamoto

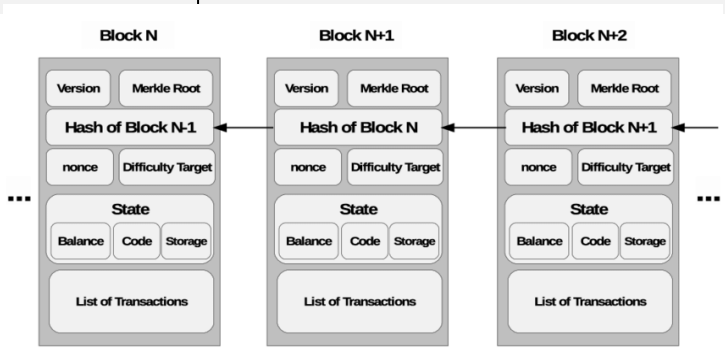
from one person ➔ one vote
to one computation ➔ one ticket (actually a scratch card)

the computation consists of making an attempt to solve a puzzle

check with some x whether H(x|A|B') has first 32 bits = 0

How do we connect blocks?

Through a soluzione of a puzzle!

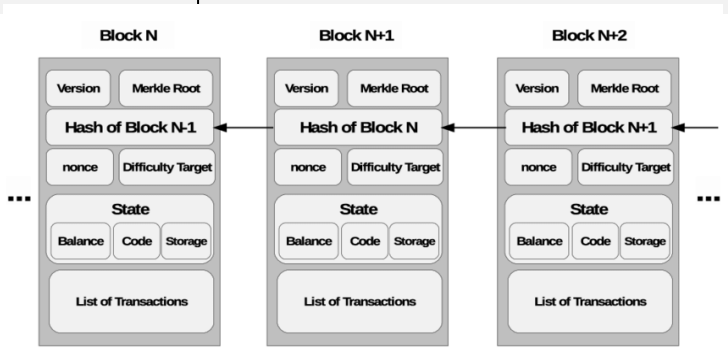


Block B=(x|B') follows block A if x
is a solution to a cryptographic puzzle derived by the content of A and B'

Cryptographic hashing can be use for this purpose:
Find x such that SHA256(x|A|B’) has the first 32 bits equal to ZERO

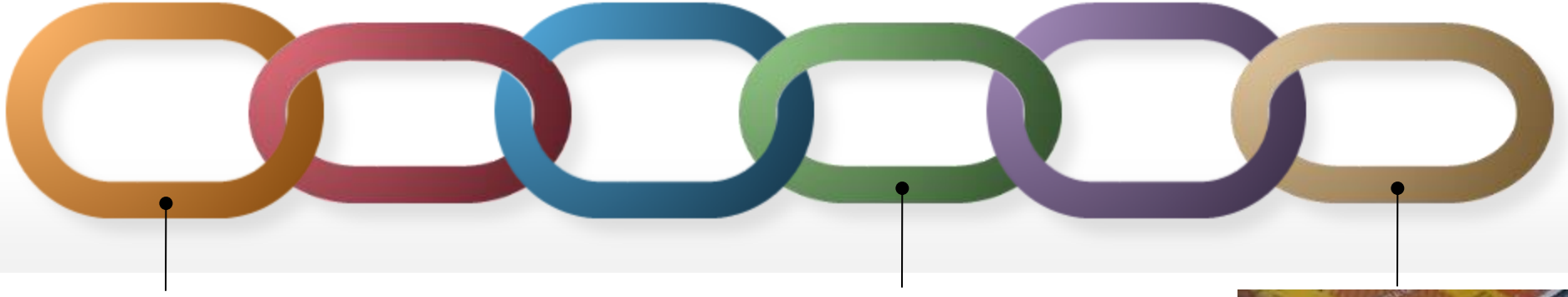
How do we connect blocks?

Through a soluzione of a puzzle!



Block B=(x|B') follows block A if x
is a solution to a cryptographic puzzle derived by the content of A and B'

Any modification to A (i.e., the past) invalidates the next blocks and it is tough to regenerate them. This comes from the modelling SHA256 as a random oracle.

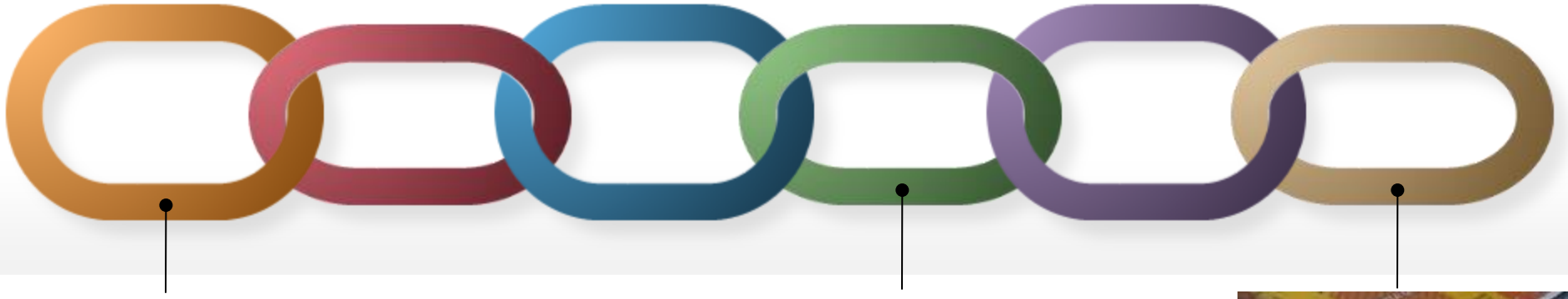


The breakthrough of Nakamoto

from one person ➔ one vote
to one computation ➔ one ticket (actually a scratch card)

no reason to talk to others, just make some computations (i.e., proofs of work) and if you win the lottery just announce it

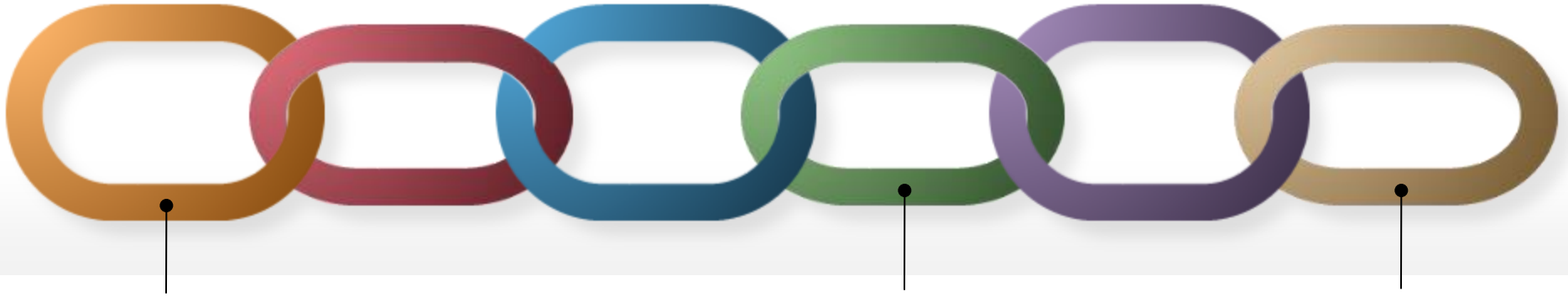
Terrific: by giving incentives you get also a huge computational power that justifies the main trust assumption: adversary has less than half of the power



The breakthrough of Nakamoto

one computation ==> one ticket (actually a scratch card)

multiple winners generate forks… the longest chain rule and the limited power of the adversary guarantee that in «the long run» all nodes will converge on the same sequence of blocks;
«the long run» is the delay to get «confirmed transactions»



Data Integrity in Blockchains: Assumptions

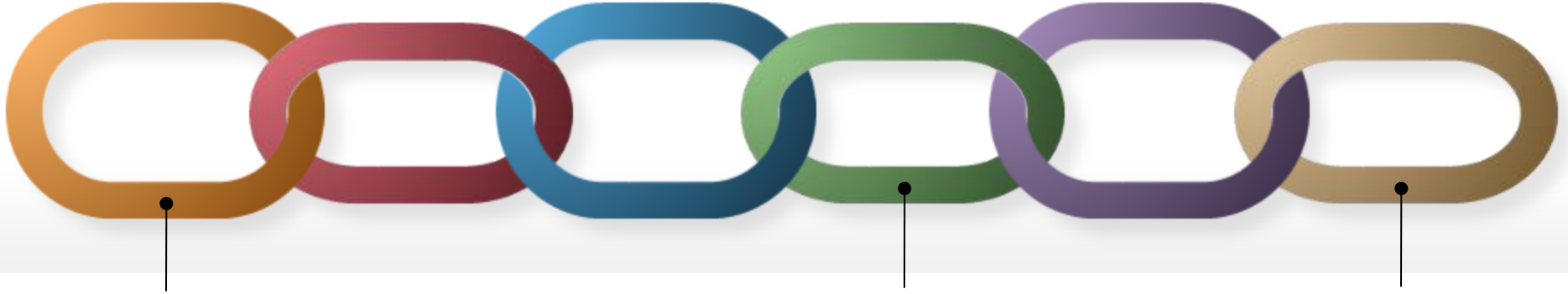
computational assumption: **collision resistance** of SHA256
find A, A' such that H(x|A|B')=H(x|A'|B')

trust assumption: if adversary has less than 50% of the computational power (supported by game-theoretic arguments associated to a reward (coins) for the solution finders) then her chains will be short (**random oracle**)

wallets imply the use of (anonymous) **digital signatures**

Consensus from Proofs of Work
- scientifically validated
- practically validated

Problem: Bitcoin is consuming a lot of energy



Environment-friendly Blockchains?

Main candidate: *Proof of Stake*

Environment-friendly Blockchains?

Main candidate: *Proof of Stake*

one coin ➔ one ticket

no waste of energy
Verifiable Random Functions do the job

VRF.Eval(SK,A,B’)=(00000…000001313223, proof)

Environment-friendly Blockchains?

Main candidate: *Proof of Stake*

one coin ➔ one ticket

intuition: security holds as long as the adversary has limited financial resources

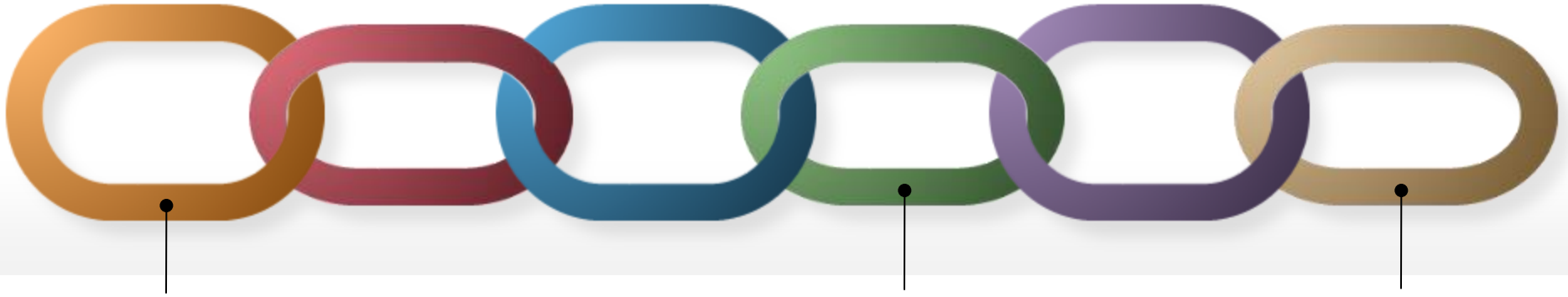
Consensus from Proofs of Stake

- pretty much scientifically validated; there are rigorous proofs but some wierd appealing assumptions to deal with specific problems (e.g., long range attack, nothing at stake attack, attack of the clones, privacy issues)
- no significant practical validation so far
- major efforts (i.e., a pile of money) in this direction

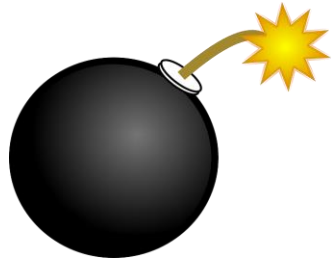
(Cardano, Dfinity, Ethereum, Filecoin, Algorand, Concordium, Snow White…)

Blockchain Technology is ready to repeat the revolution of the Internet?

Internet has been secured using standard cryptographic tools that are instead insufficient for privacy in blockchains



Public Verifiability vs Data Removal



removing a transaction could **invalidate** many smart contracts since their states could not be verifiable anymore.

Why should we remove data from a blockchain?

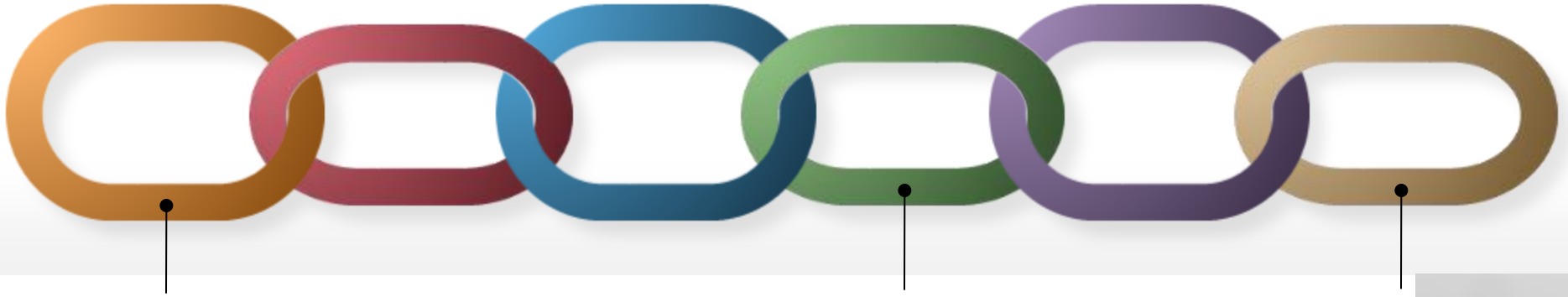
Example: Bitcoin Blockchain

in the Bitcoin blockchain there are links to child pornography

Child abuse imagery found within bitcoin's blockchain

Researchers discover illegal content within the distributed ledger, making possession of it potentially unlawful in many countries

theguardian.com



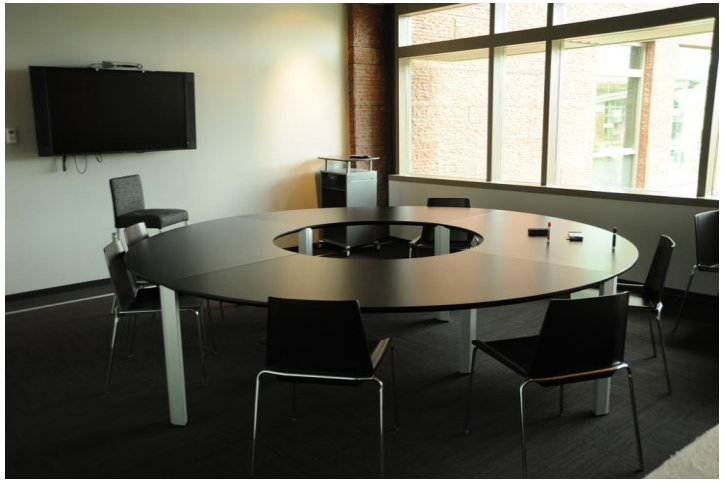
Can we remove data from a Blockchain?

the only way to do it is to contradict the underlying assumption (e.g., honest majority of partipants, of computing power, of stake possession,…)

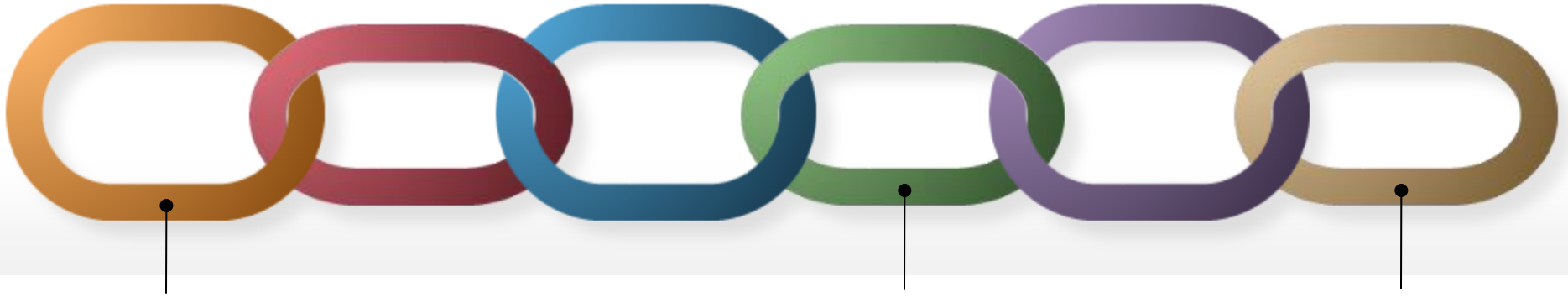
but do we really need immutability? (no…)

Permissioned Blockchain (State-Machine Replication)

mutually distrustful known organizations manage the blockchain (recall: 1 person ➔ 1 vote)



- no waste of energy
- fast consensus
- no need of tokens/incentives
- immutability guaranteed by honest majority



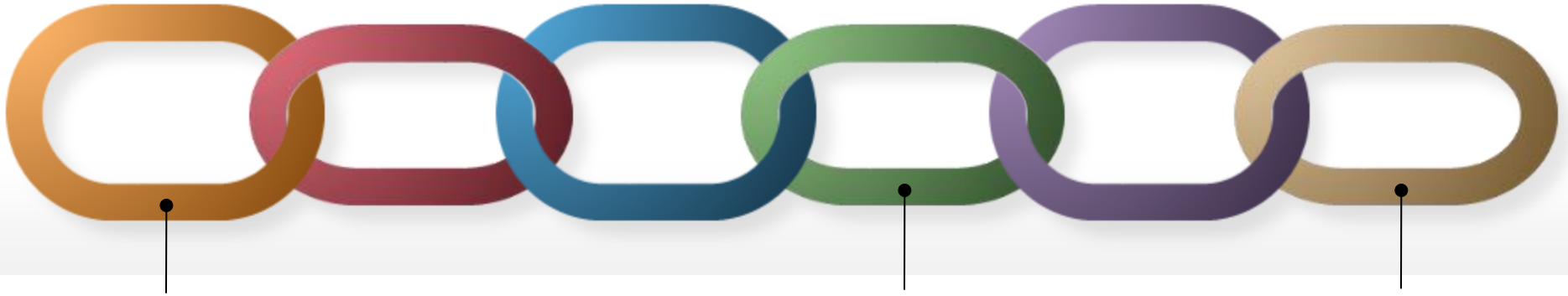
You might want to use a Blockchain every time you are afraid of cheating

- e-voting, supply chain
- lotteries, games
- or more generically: any problem trivially resolved with the help of a trusted third party
- it makes sense only if all actors involved in the process believe in a honest majority among consortium members

Do you see any problem?
What about privacy?

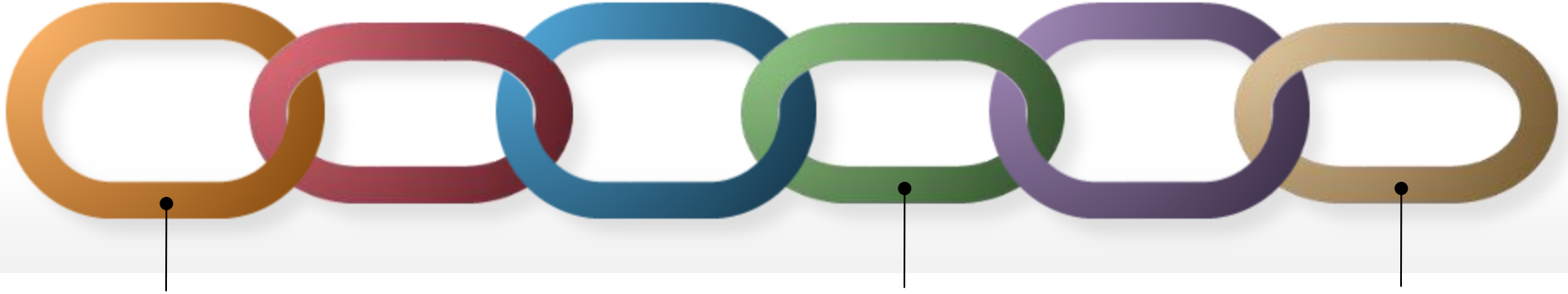
it does not seem that you can have public verifiability/transparency along with privacy

how can we use the integrity of a blockchain still preserving privacy?



Two major goals in Cryptography

- Data Integrity
- Data Confidentiality



Common ERRORs

naive

Upload on a blockchain just a cryptographic hash of confidential data.

Problem: hashing does not hide enough.
Solution: a **commitment scheme** (i.e., SHA256(r|m)) would work but sending r and m can be devastating for privacy.

Blockchain: Privacy and GDPR

are immutability, public verifiability and confidentiality compatible with current (and future) GDPR?

Zero-Knowledge Proofs [GMR85]

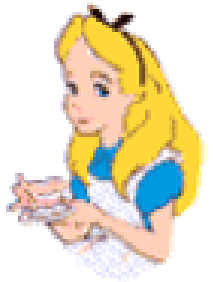
Use advanced cryptography to relax the tension between public verifiability and privacy

E.g.: Zero-Knowledge Proof
Prove that something is true without revealing any other information (e.g., put commitment on the blockchain and prove in zero knowledge that m is inside the commitment)

Example

Claim: I can distinguish an original painting from an imitation

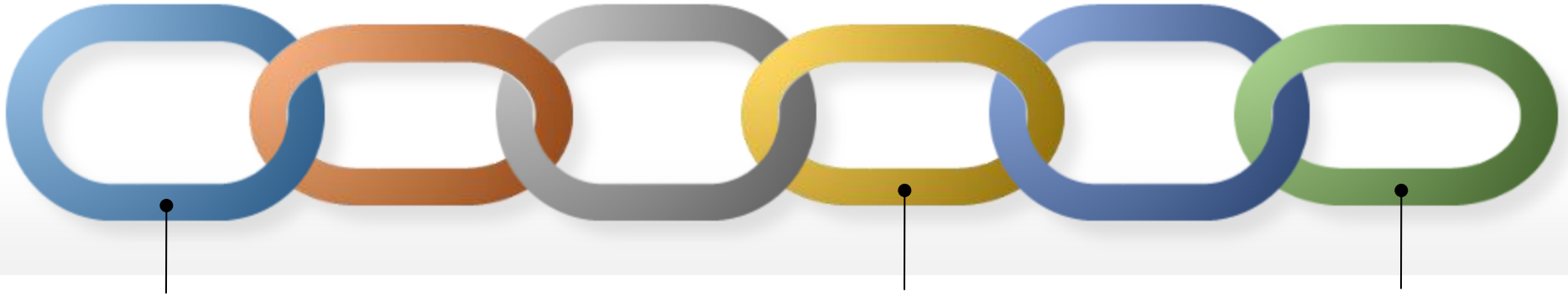
0/1



0

1

if Claim is true then answer is correct otherwise high chances to be caught

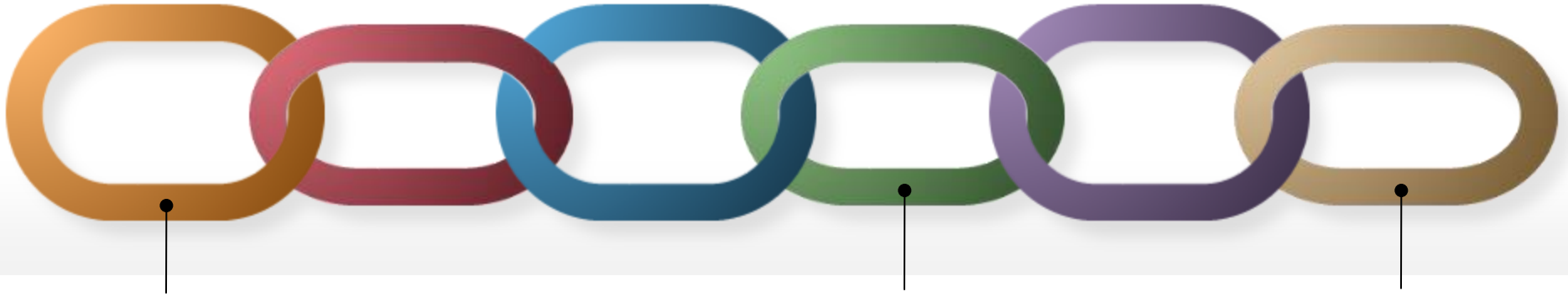


ZK Proofs

It’s not just theory, they are very efficient for several useful claims.

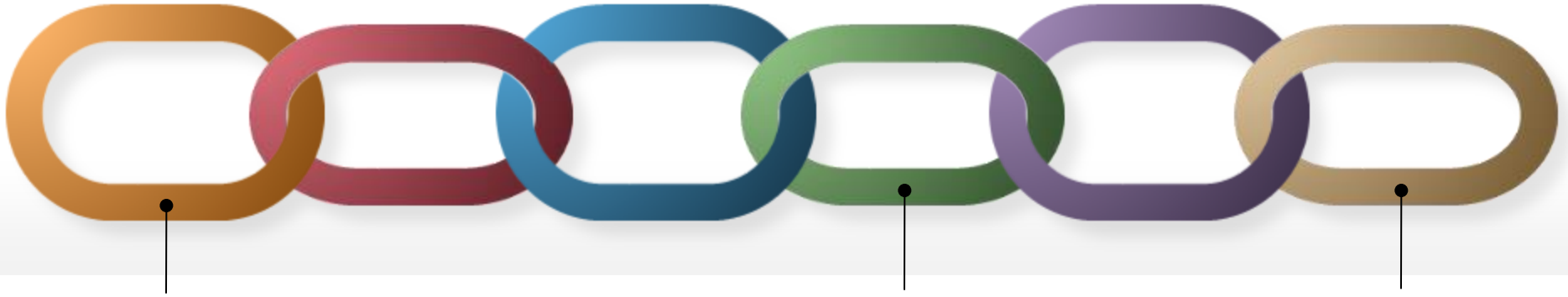
They can even be succinct (i.e., small length for proving a claim about the entire blockchain!) and are used in ZCash

some names getting popular: zk-SNARKS, zk-STARTKs…
make sure you don’t play too much with fire…



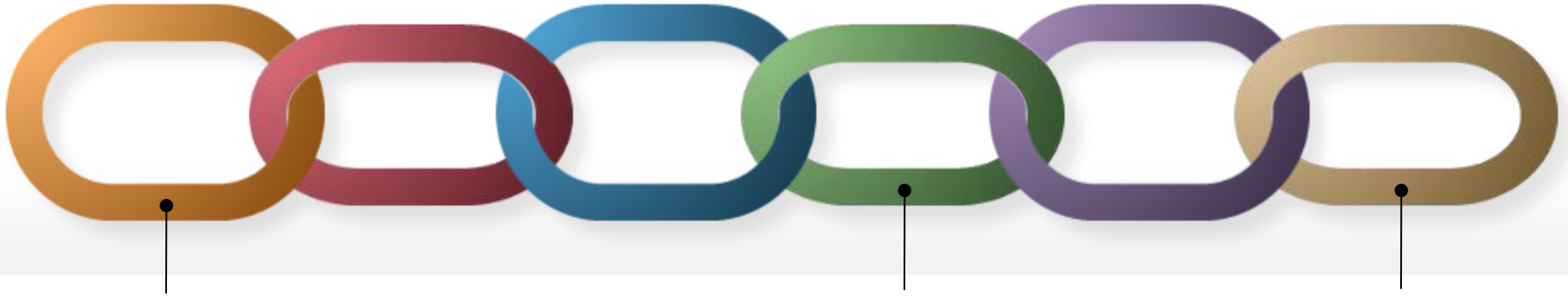
Blockchain and the Physical World

how can a blockchain be useful (e.g., against counterfeating) w.r.t. the physical world?



Blockchain and the Physical World

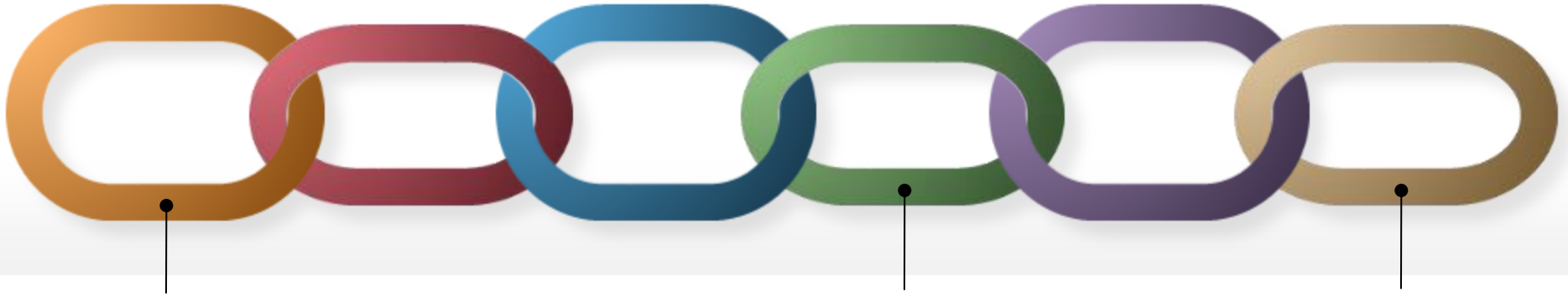
don’t expect that Blockchain Technology alone will resolve all problems



The bridge between physical and digital assets

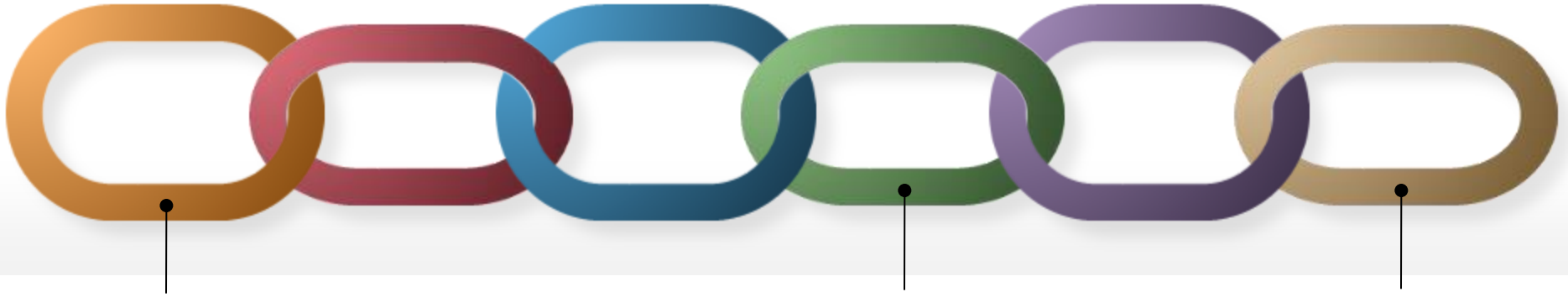
a physical asset should have a «secure» digital representation

this needs to be done without the help of blockchains, some external certification is needed



The bridge between physical and digital assets

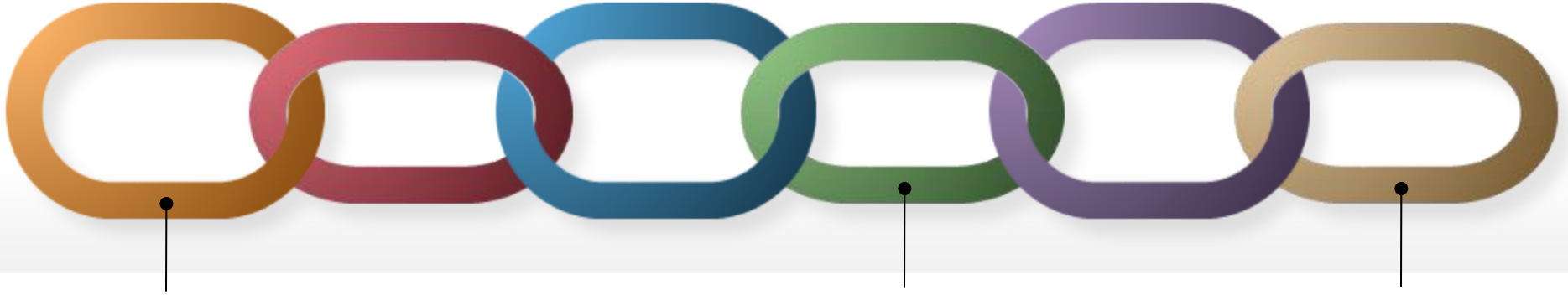
example: it’s always possible to put cheap wine into an empty 100 Eur bottle of wine, so blockchains alone can’t resolve the problem of the food supply chain



The bridge between physical and digital assets

example: it’s always possible to put cheap wine in an empty 100 Eur bottle of wine, so blockchains alone can’t resolve the problem of the food supply chain

idea: use a «secure» electronic/physical seal (e.g., through RFID, physically unclonable functions, etc..)

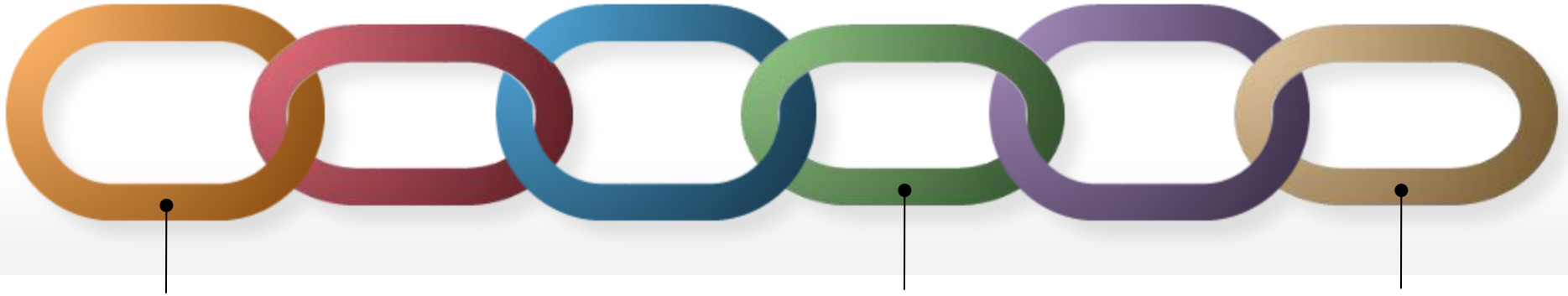


The bridge between physical and digital assets

example: it's always possible to put cheap wine in an empty 100 Eur bottle of wine, so blockchains alone can't resolve the problem of the food supply chain

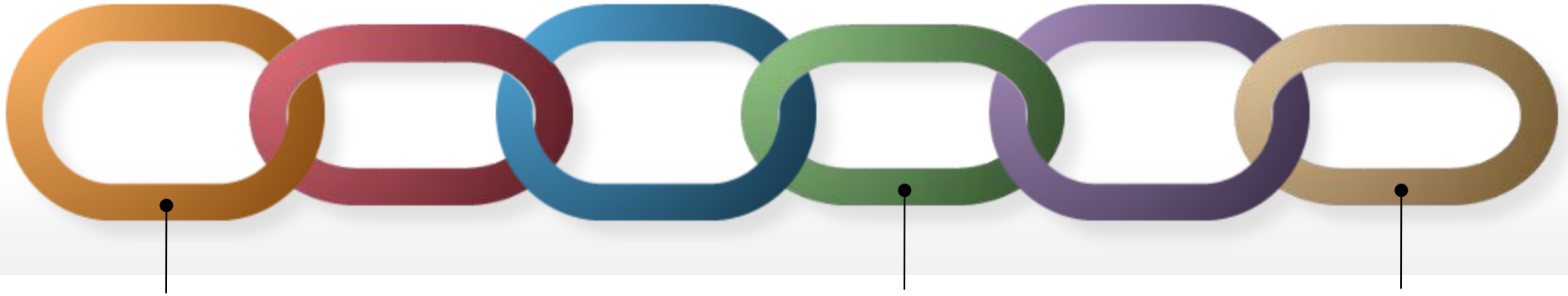
idea: use a «secure» electronic/physical seal (e.g., through RFID, physically unclonable functions, etc..)

you must identify the adversary in your application… it's about defining the **security model**….still a job for a cryptographer!
(have a look at secure multi-party computation)



Conclusion

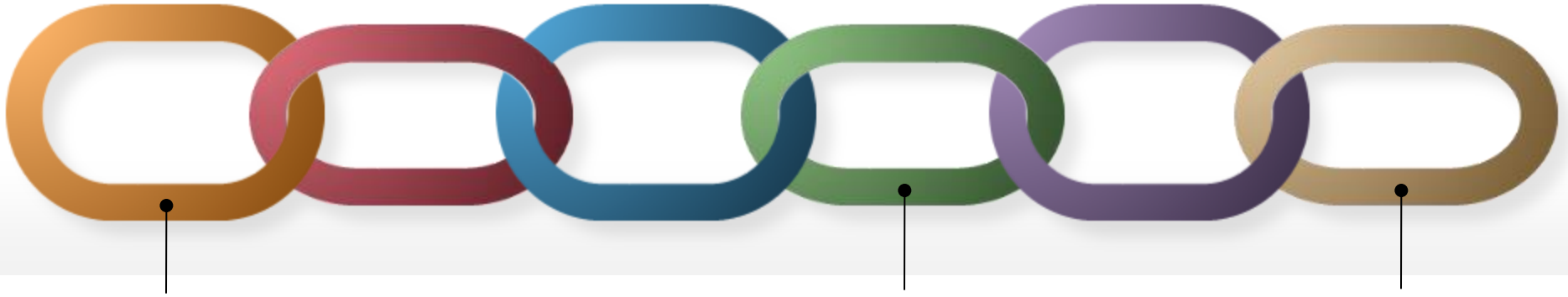
Blockchain technology is a powerful tool against counterfeating, it allows to relax the need of trusted third parties and can have a strong impact on our societies.



Conclusion (the good side)

Many interesting challenges for scalability, security, decentralization, incentive mechanisms, confidentiality, connections to the physical world and compliance to laws.

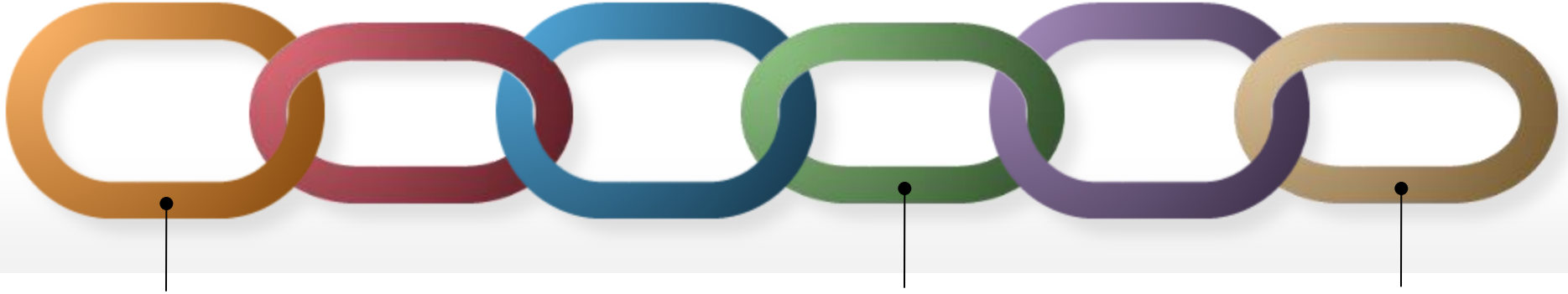
It’s a gold mine for a cryptographer (and more).



Conclusion (the ugly side)

A lot of noise from self-appointed blockchain evangelists, many scammers, several developers unaware of what they are doing, everyone wants to do/produce nobody wants to think/study enough.

Very few real experts around…



Thank you for your attention!

visconti@unisa.it