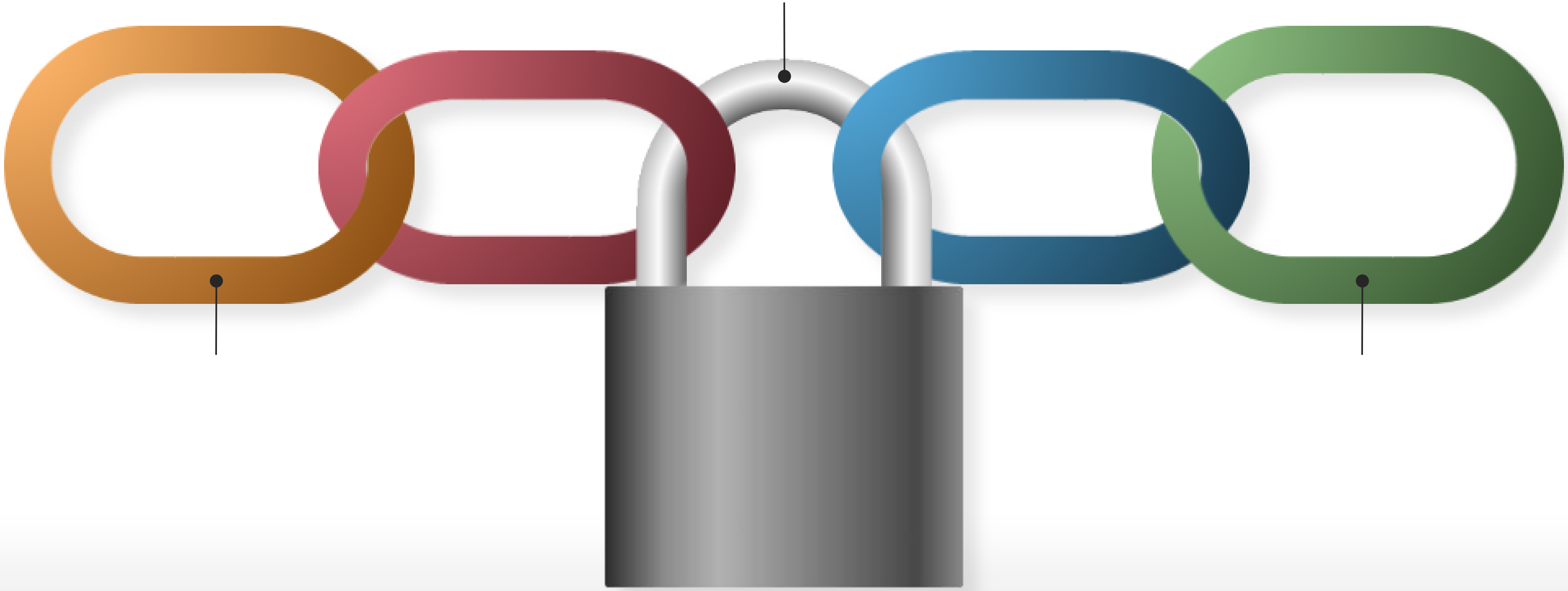
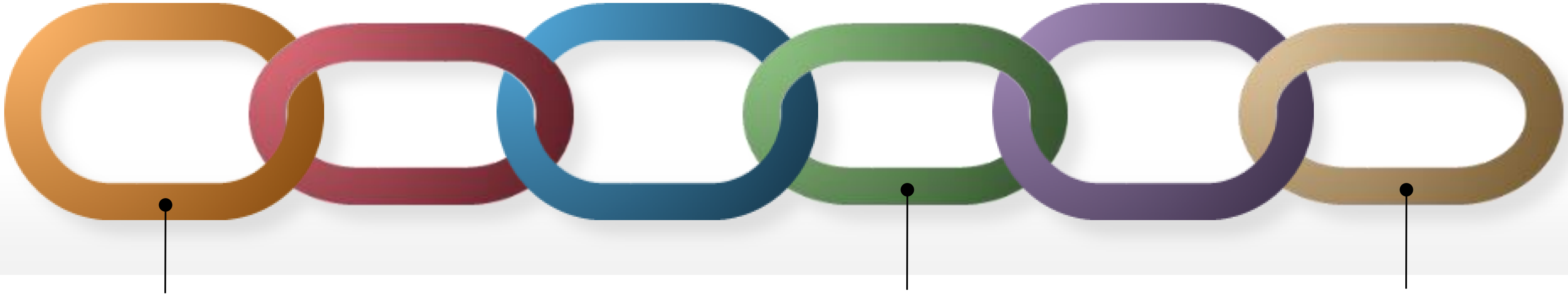


On Deleting Data from a Blockchain

(towards GDPR compliance and more…)

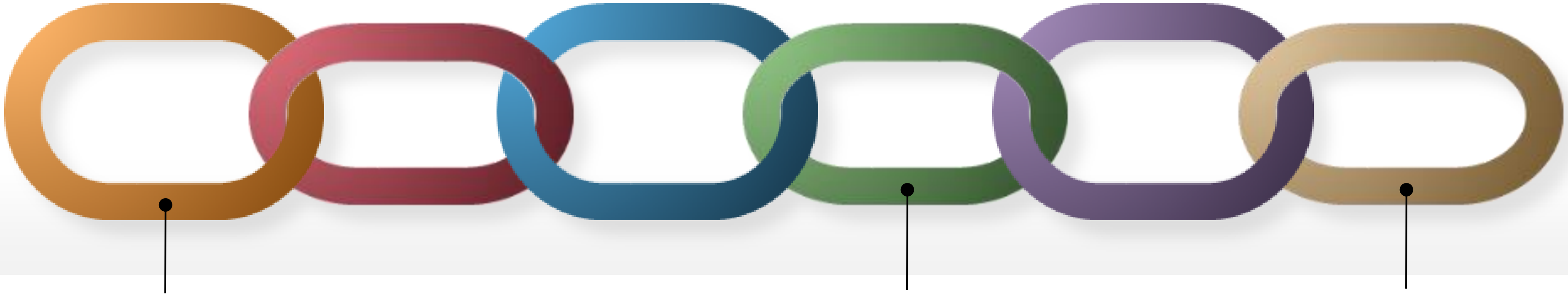
Luisa Siniscalchi and Ivan Visconti

DIEM, Università di Salerno



Ivan Visconti

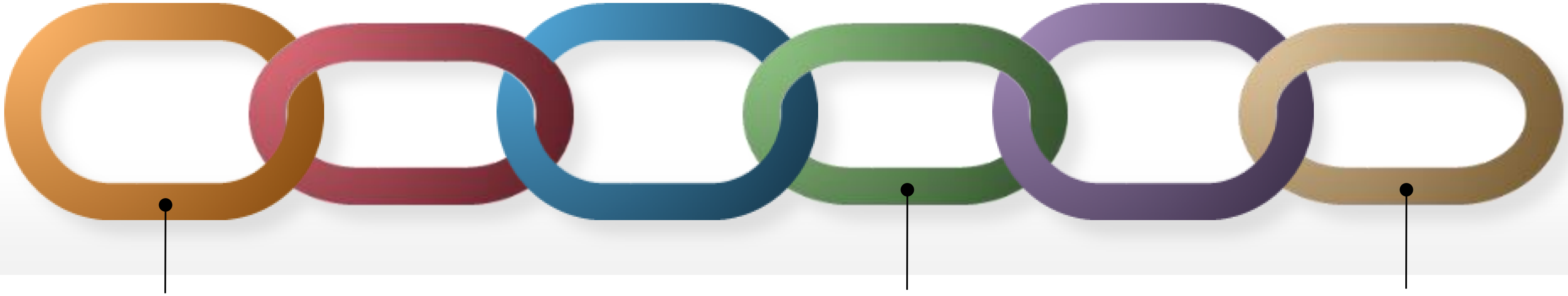
- Prof. of Computer Science, Università di Salerno (DIEM)
- Coordinator of CifrisChain (Blockchain group inside De Cifris)
- Scientific coordinator for Univ. of Salerno of EU-H2020 PRIViLEDGE



Blockchain

a blockchain is a **decentralized** platform that through validations of transactions allows to update the state of processes that correspond to the executions of smart contracts

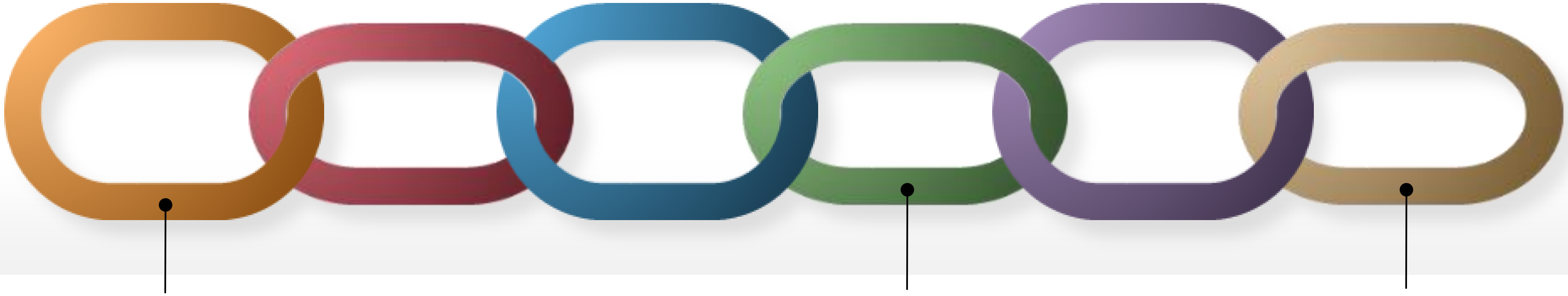
updates are **irreversible** (data immutability)



Decentralized Blockchain: Public Verifiability

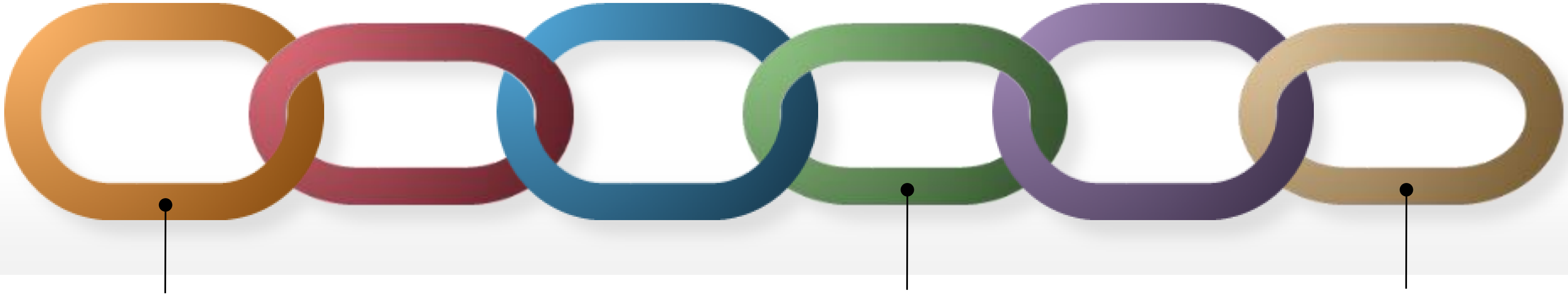
a main reason behind the success of this technology is that everyone can check the evolution of a process, from the initial state to the current state

:



Decentralized Blockchain – ~~Public Verifiability~~

by removing a single transaction, an entire process becomes untrusted

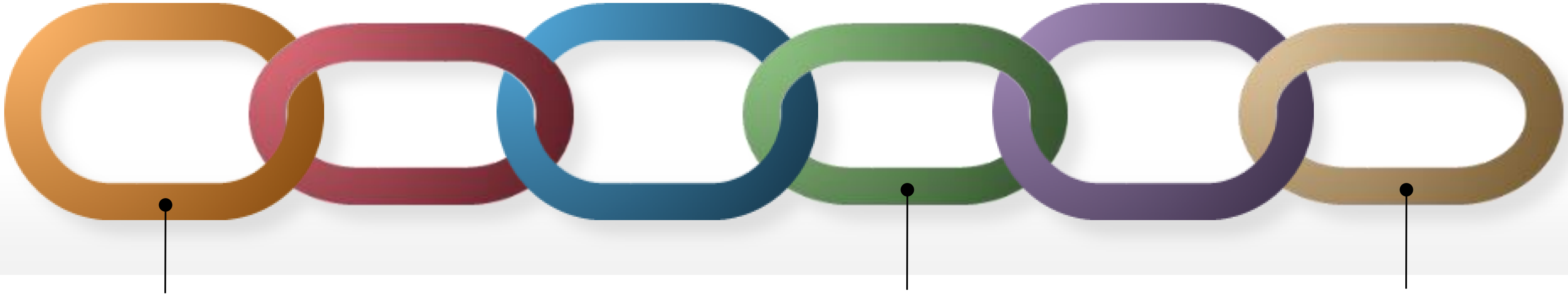


Decentralized Blockchain – Privacy and GDPR

is data immutability compatible with privacy regulations (e.g., GDPR)?

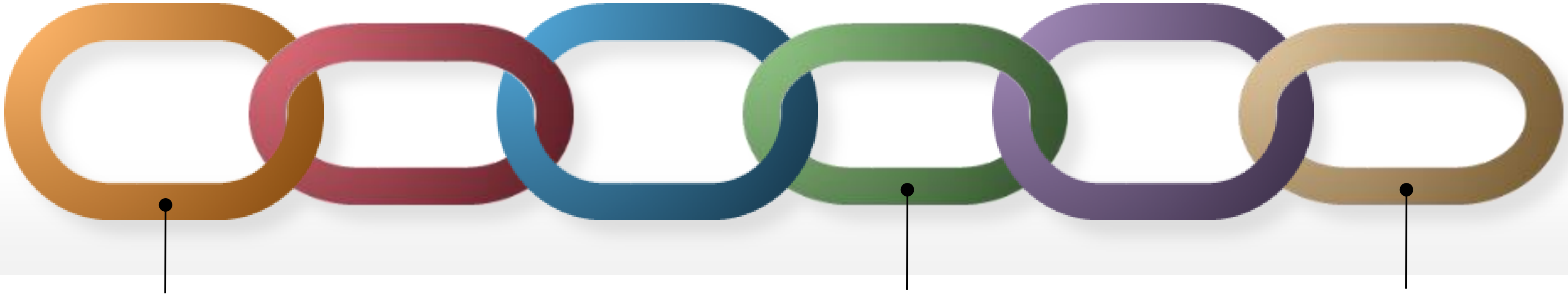
Yes and No

…it depends…



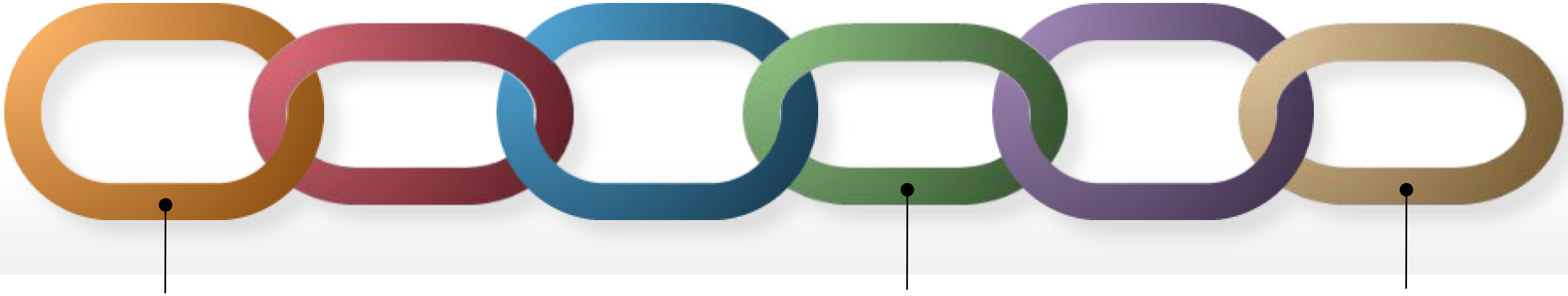
Common belief: only hashes are chained

the chaining in common blockchains is applied only to cryptographic hashes of actual data, therefore removing data does not affect the chaining



False expectation: only hashes are chained

a blockchain is not just a log of uncorrelated data, it is an history of the executions of processes that must be verified in order to have decentralized trust

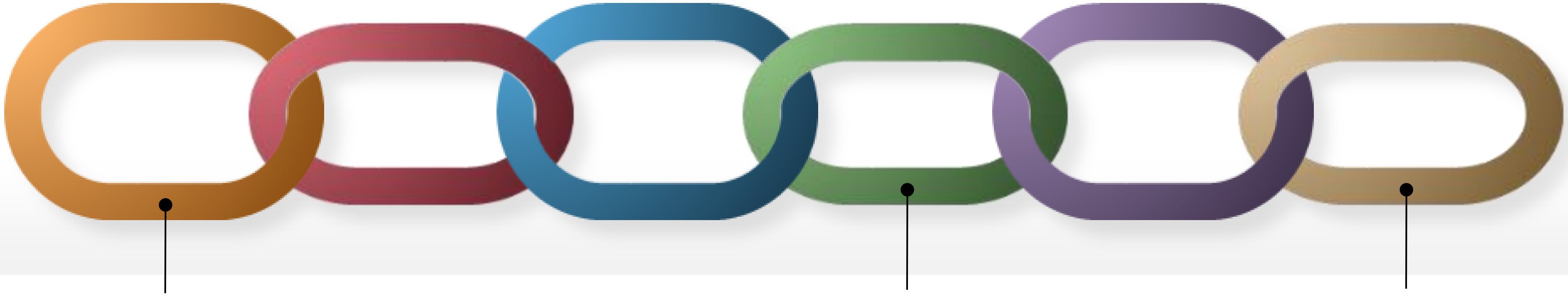


What is data removal in a Blockchain?

it's a replacement of data contained in a block

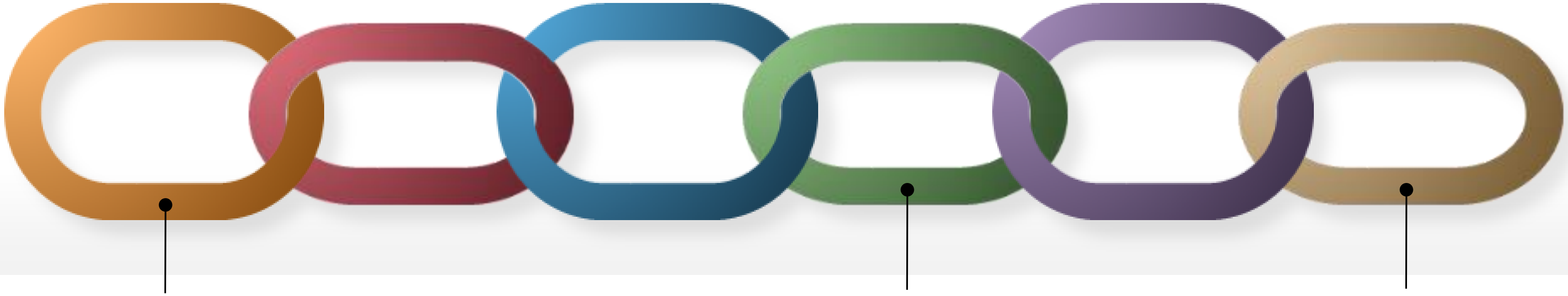
data immutability requires that data removal must be hard under some chaining assumptions

(on the computational power, stake, corruption…)



CASE 1: Permissioned Blockchains

what is the «chaining» assumption?



CASE 1: Permissioned Blockchains

what is the «chaining» assumption?

honest majority of the organizations in the consortium

CASE 1: Permissioned Blockchains

can we remove data?

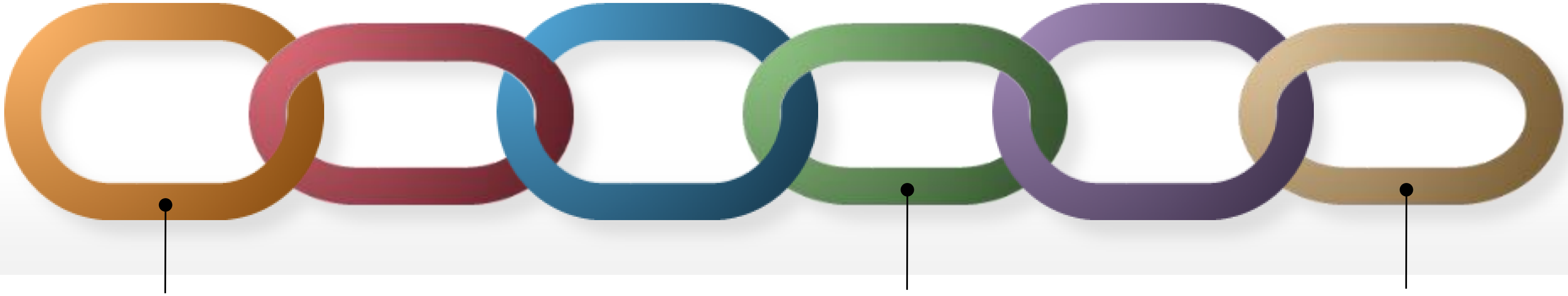
YES, of course! and it is **trivial**! it’s enough that a majority agrees on it…. details in the next slides

CASE 1: Permissioned – n organizations

implement the chaining with n/2+1 signatures from n/2+1 organizations

the signed message consists of: transactions + the index of the block

replacing a block with index i: just sign a new block with the same index **DONE!**



CASE 1: Permissioned – compactness

implement the chaining with n/2+1 signatures from n/2+1 organizations

is the signature too long?

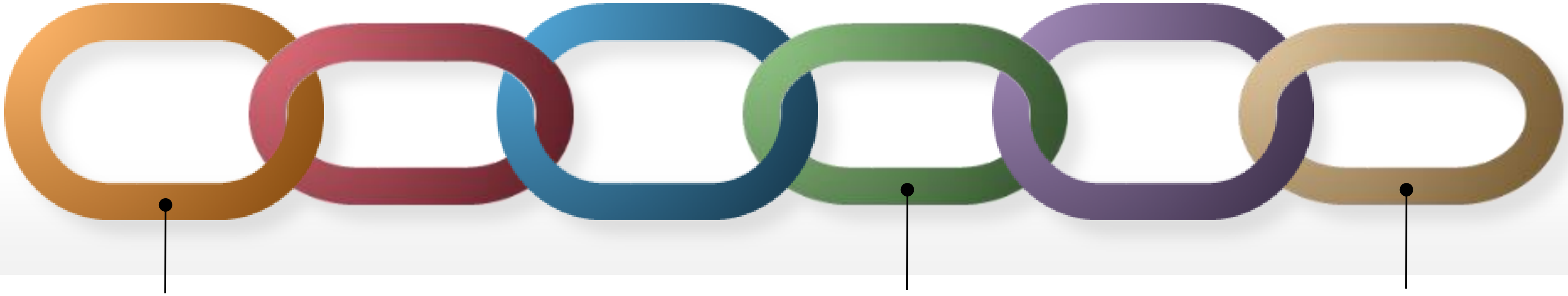
just use threshold signatures and you get a compact signature through n/2+1 contributions, **DONE!**

CASE 1: Permissioned – previous work

is it really so trivial? so why did others invent new primitives and sophisticated mechanisms to achieve it?

CASE 1: Permissioned – just make up

something is fishy…. blockchains are immutable and now we can trivially remove data



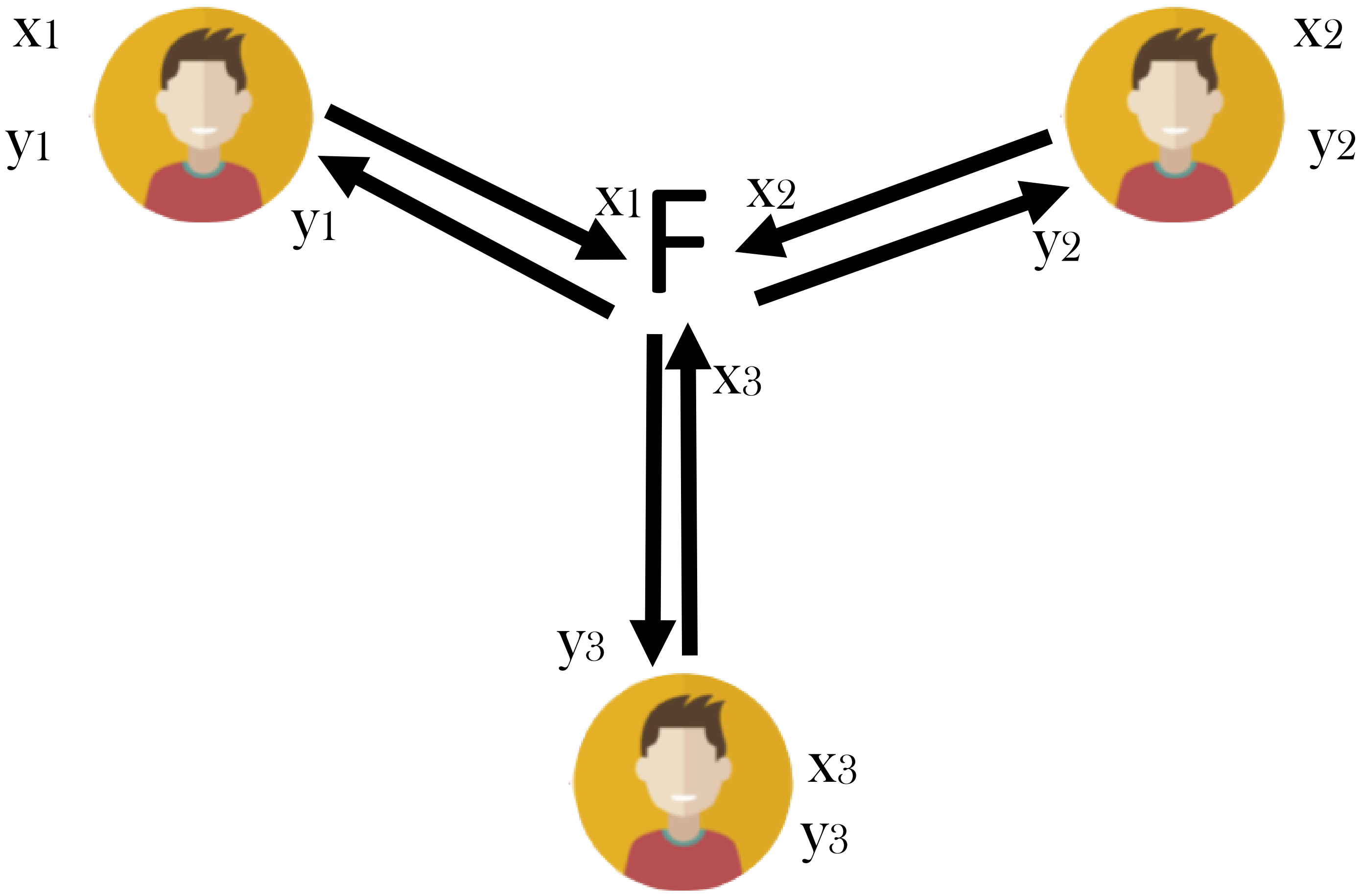
CASE 1: Permissioned – the truth is……

something is fishy…. blockchains are immutable and now we can trivially remove data

the point is that there is confusion between real blockchains (i.e., permissionless) and «masked» blockchains (i.e., permissioned)

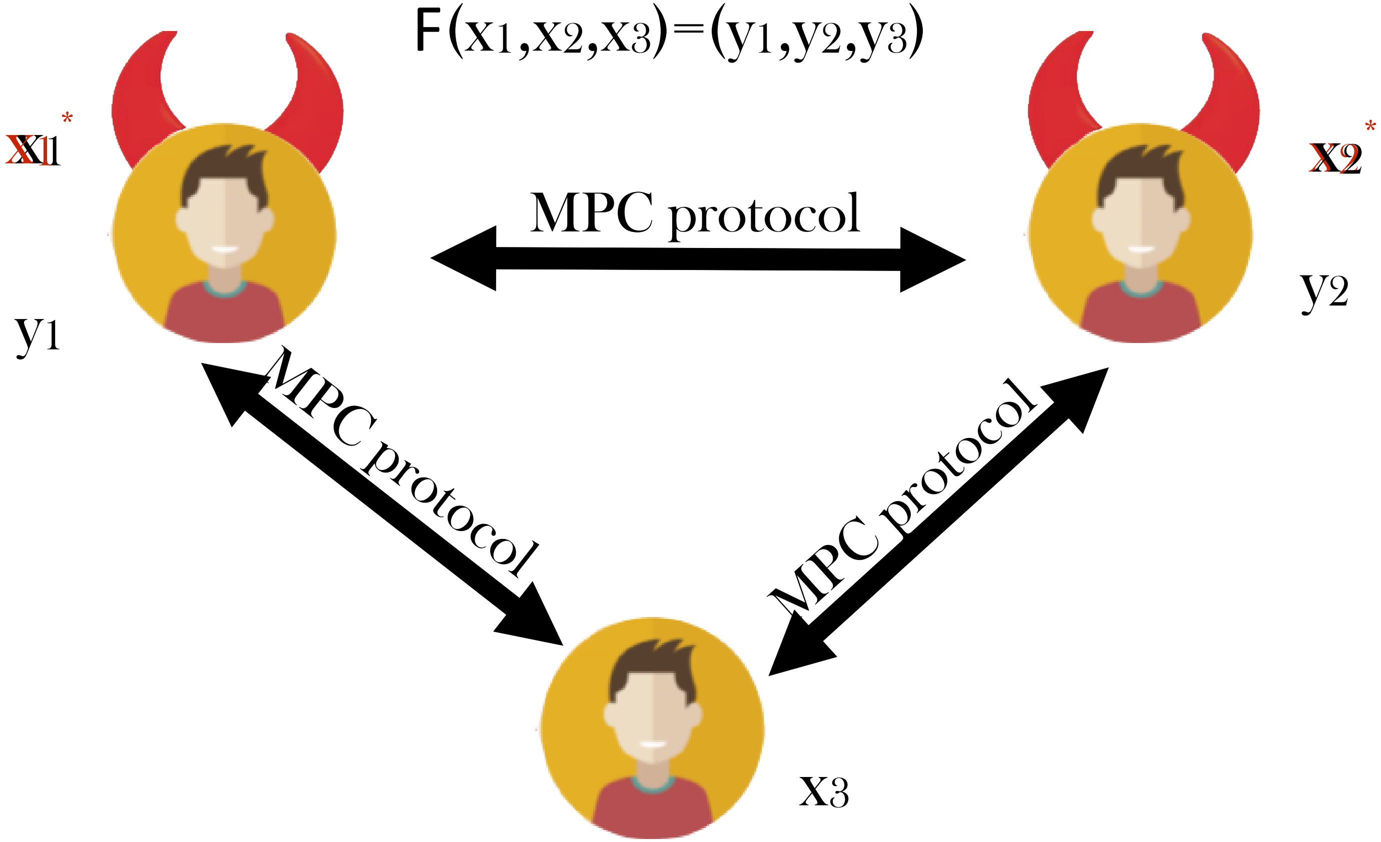
Multi Party Computation (MPC)

$F(x_1,x_2,x_3)=(y_1,y_2,y_3)$



Multi Party Computation (MPC)

$F(x_1,x_2,x_3)=(y_1,y_2,y_3)$



x_1 x_1^*

MPC protocol

x_2 x_2^*

y_2

y_1

MPC protocol

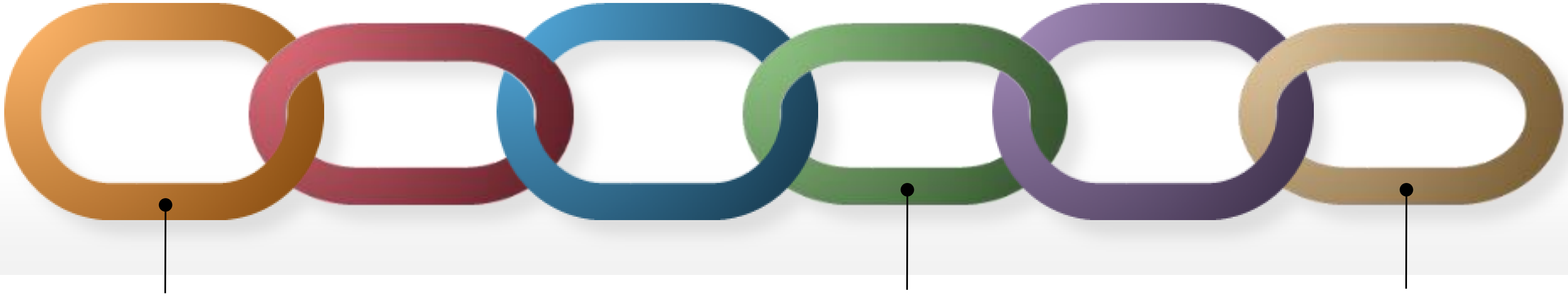
MPC protocol

x_3

y_3

Correctness

Security (input-output privacy is preserved)

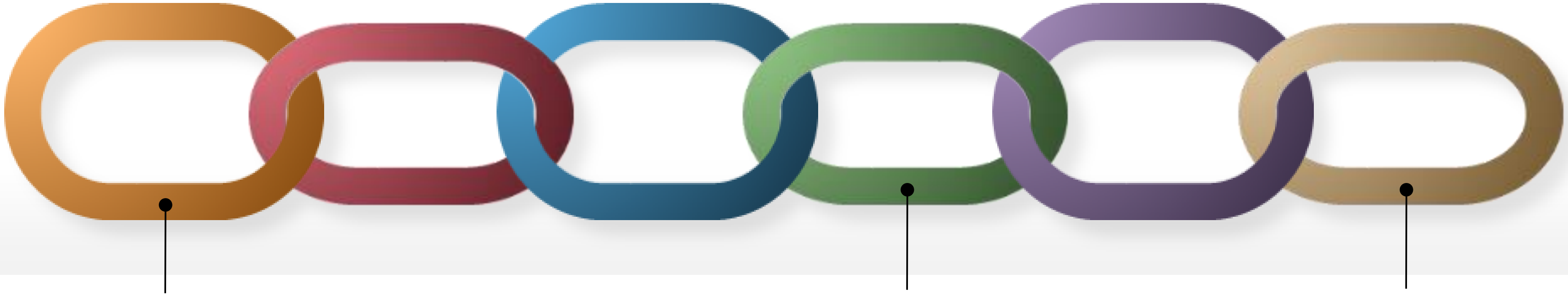


CASE 1: Permissioned – the truth is…

permissioned blockchains are well known objects

it is «secure multi-party computation» (MPC) with a mask just to exploit the blockchain hype

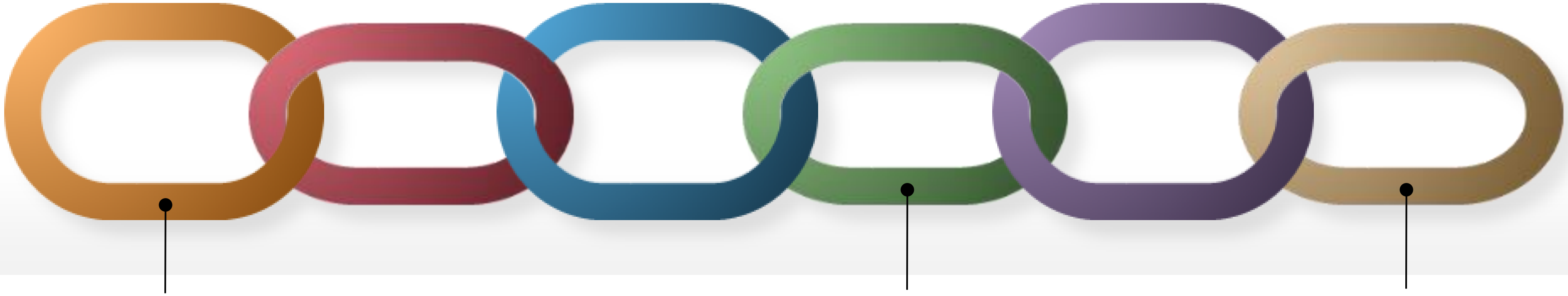
experts of MPC know about it but keep it under the rug



CASE 1: Permissioned – just MPC

permissioned blockchain is a specific case of MPC

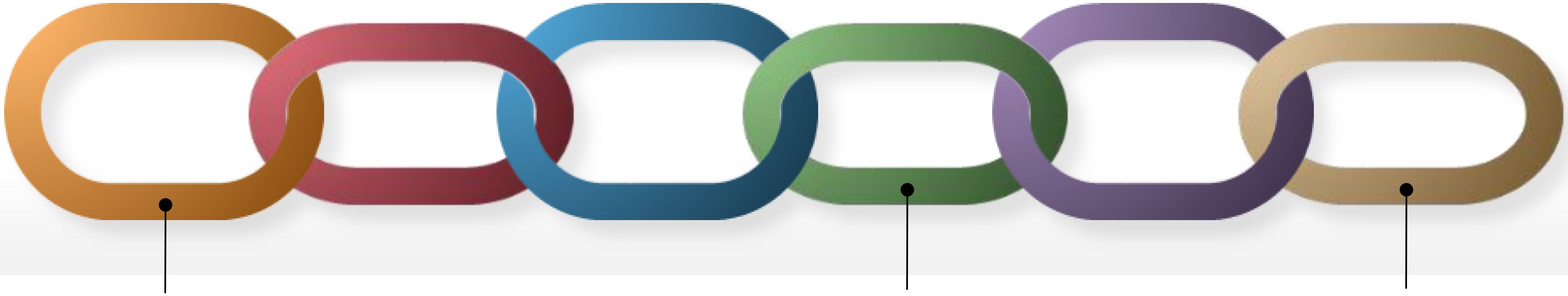
if you need to customize the behavior of a permissioned blockchain (e.g., allowing data removal or other features), just refer to an expert of MPC



CASE 2: Permissionless (Nakamoto's) Setting

here date removal is tough; there is no honest majority and therefore MPC is useless

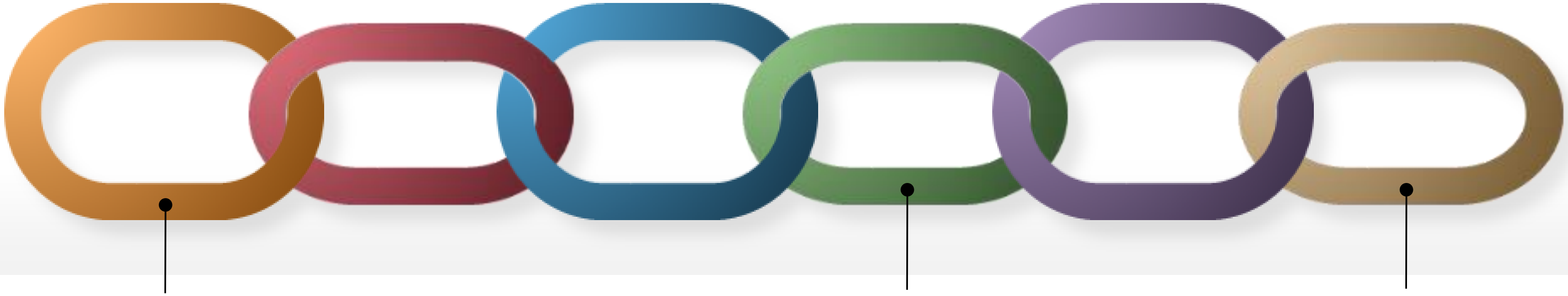
the feeling that removing data should not be possible is correct, in general: just give up!



CASE 2: Bitcoin Blockchain

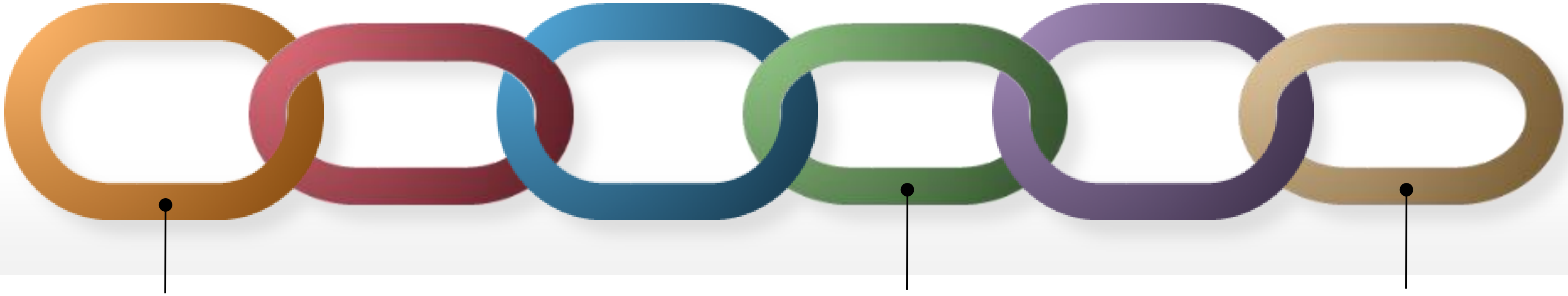
warning: in the Bitcoin blockchain there are some links to child pornography

can Bitcoin (as it is) survive to data removal requests?



CASE 2: how can data storage be forbidden?

data is just a sequence of bits that are stored in different ways, through some enconding



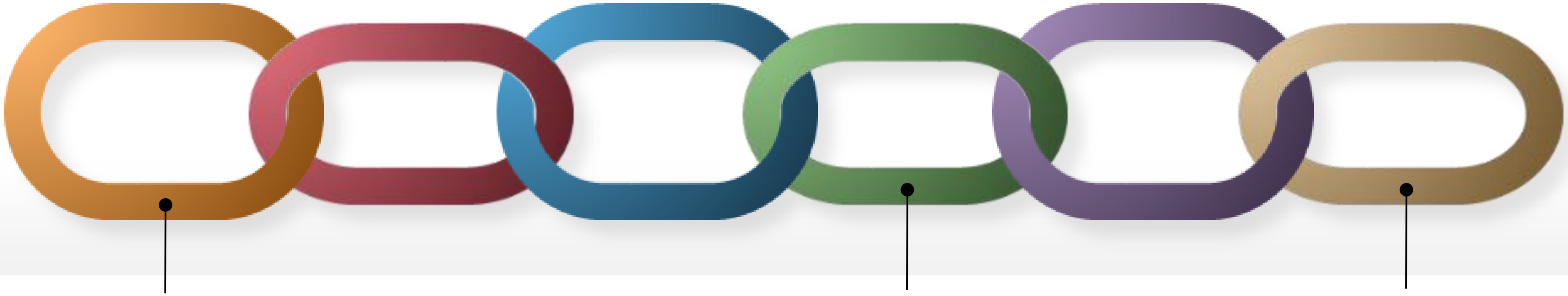
Playing with Interpretations of GDPR

GDPR compliance could be possible by just making data unavailable to applications, but still allowing its storage for the consensus

this is work for lawyers… we are available to assist them

Perhaps Another Gift from Blockchains

the tension between data removal and immutability of blockchains might give us a more reasonable interpretation of illegal data possession



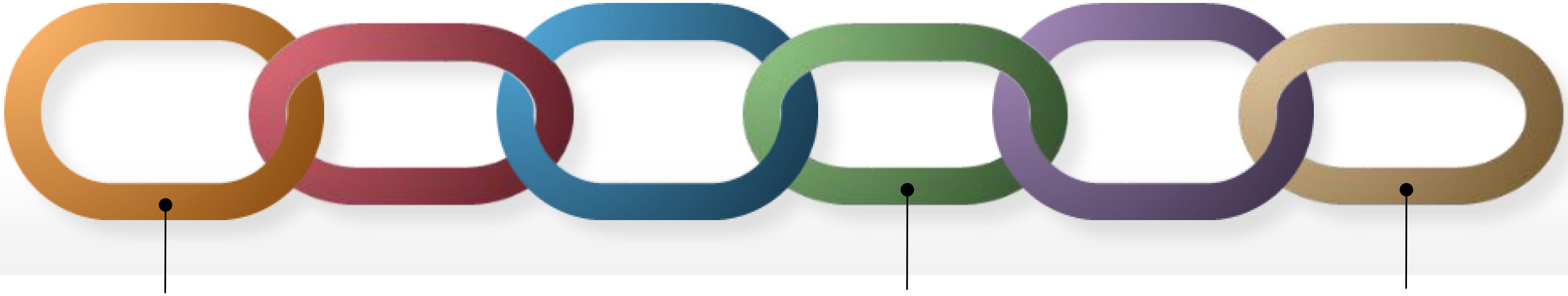
CASE 2: back to Nakamoto’s setting

removing the past is hopeless, but with hard forks we could have a better future

CASE 2: Bitcoin*

split a transaction in two shares, one with full data, one only about currency exchange from (well formed) wallets to (well formed) wallets

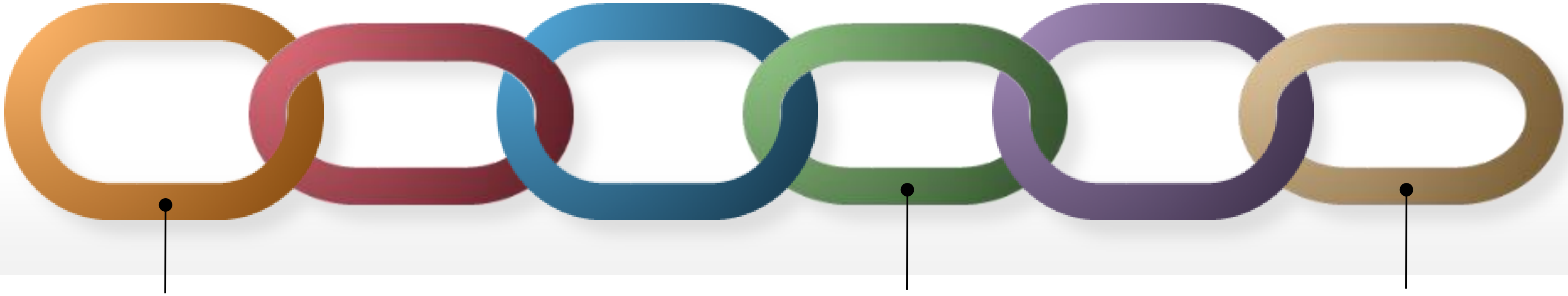
later on you can safely remove the first share



CASE 2: playing with laws

keep in the system 2 replications each with zero information about transaction data (one-time-pad style), and full information about chaining

consistency is achieved, locally nothing forbidden is stored, new nodes can bootstrap by combining both replications, having for short time the illegal information



Conclusion

many apparently unbreakable barriers related to blockchain technology can be demolished through a synergy of experts in law, cryptography, cryptocurrencies, cybersecurity, smart contracts, game theory and more…

maybe the main open problem is to force them to talk to each other