BLOCKCHAIN&LRs

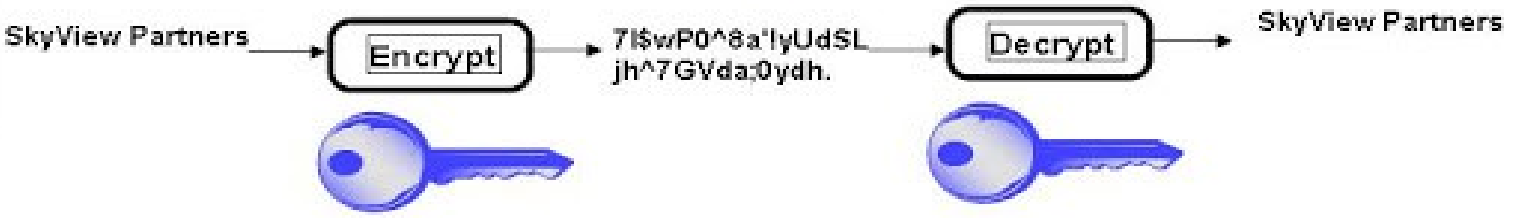
- Introduction
- Key elements BC
- SC
- Should we use it?
- Principles-Projects

Types of Encryption

DES
TripleDES
AES
RC5

Symmetric Keys

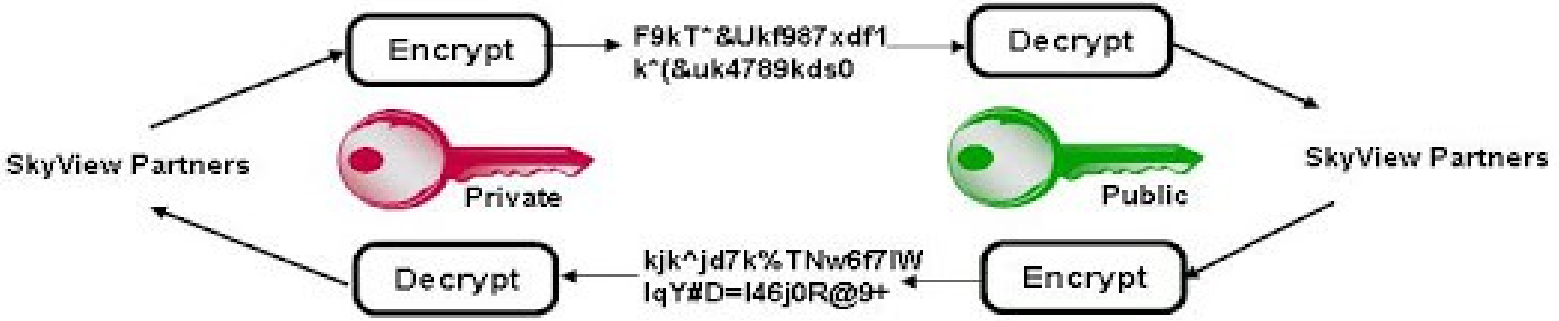
- Encryption and decryption use the **same key**.



RSA
Elliptic Curve

Asymmetric keys

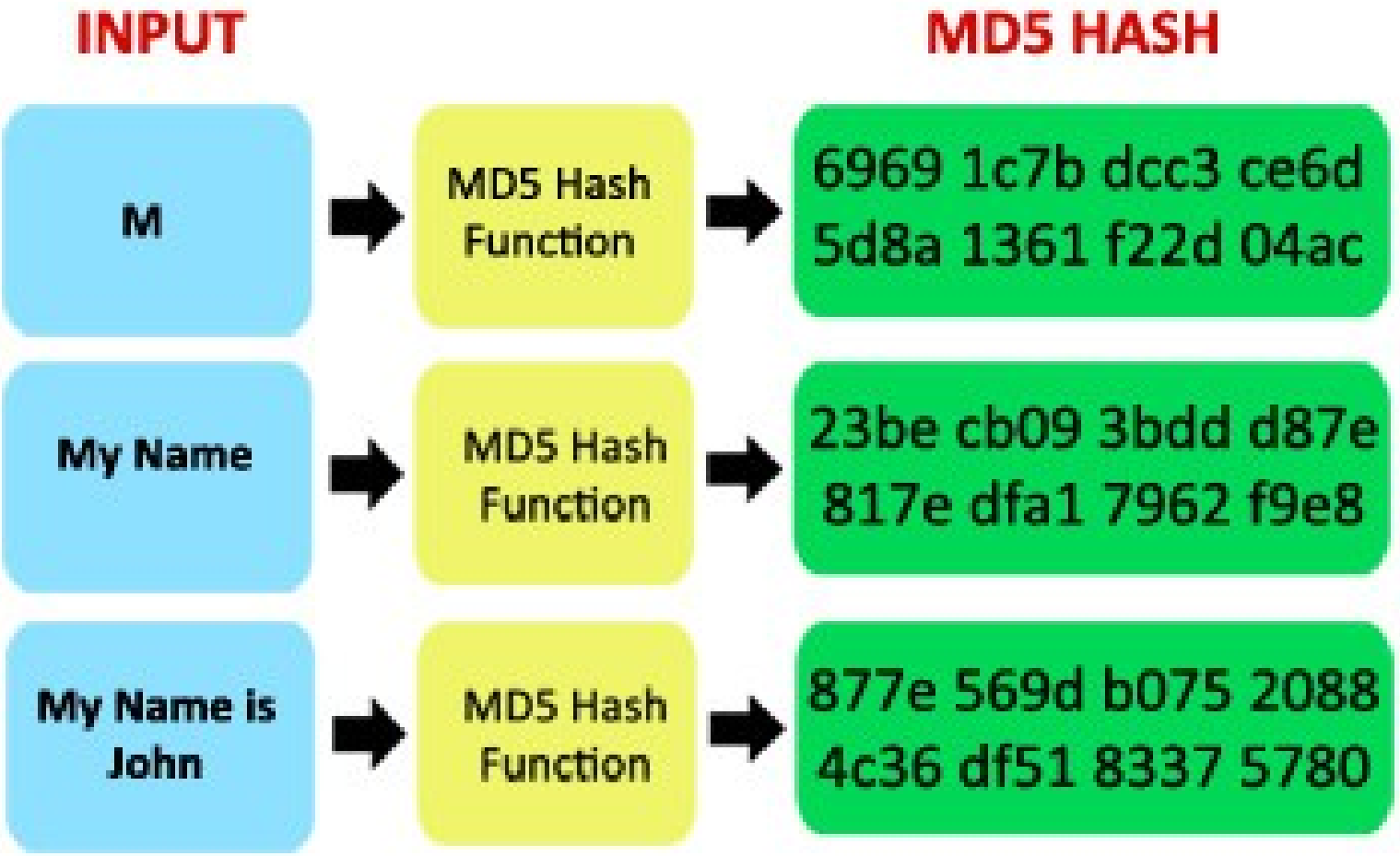
- Encryption and decryption use different keys, a **public key** and a **private key**.



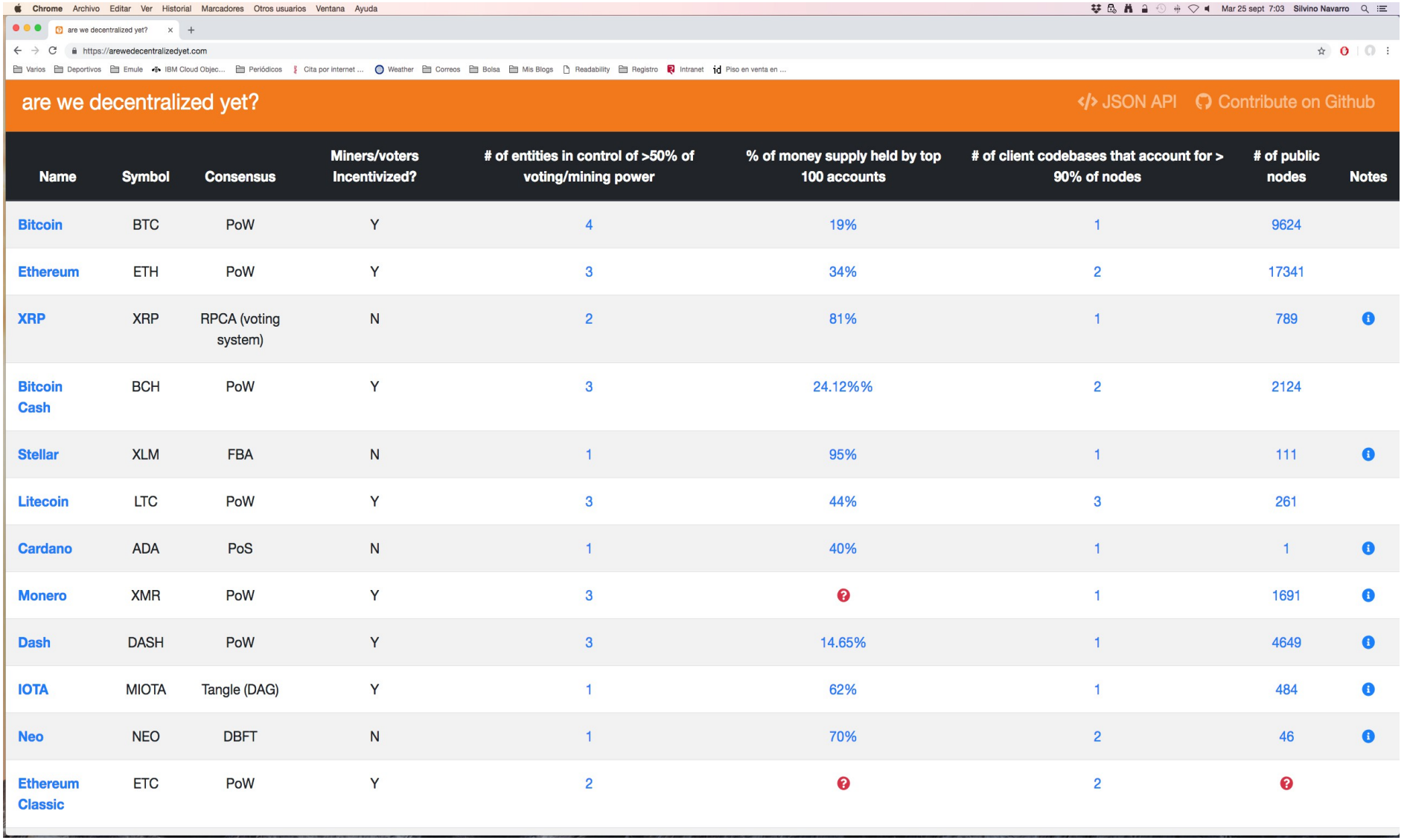
MD5
SHA-1

One-way hash

MD5 Hashing Algorith



Are we decentralized yet?



are we decentralized yet?

JSON API Contribute on Github

Name	Symbol	Consensus	Miners/voters Incentivized?	# of entities in control of >50% of voting/mining power	% of money supply held by top 100 accounts	# of client codebases that account for > 90% of nodes	# of public nodes	Notes
Bitcoin	BTC	PoW	Y	4	19%	1	9624	
Ethereum	ETH	PoW	Y	3	34%	2	17341	
XRP	XRP	RPCA (voting system)	N	2	81%	1	789	
Bitcoin Cash	BCH	PoW	Y	3	24.12%%	2	2124	
Stellar	XLM	FBA	N	1	95%	1	111	
Litecoin	LTC	PoW	Y	3	44%	3	261	
Cardano	ADA	PoS	N	1	40%	1	1	
Monero	XMR	PoW	Y	3	?	1	1691	
Dash	DASH	PoW	Y	3	14.65%	1	4649	
IOTA	MIOTA	Tangle (DAG)	Y	1	62%	1	484	
Neo	NEO	DBFT	N	1	70%	2	46	
Ethereum Classic	ETC	PoW	Y	2	?	2	?	

Smart Contracts

Nick Szabo :*“a set of promises, specified in digital form, including protocols within which the parties perform on the other promises”*

Vending Machine

SC are self suficient. Doesn't need the suport of the state

SC questions

- Binding vs Automatic Execution
- Who signs? Is he really him? Minor?
- Fully understands? Informed?
- Freedom ways of contract
- Digital breach
- Are we going to standard contracts? Do we want that?
- Who writes them? Responsability. DAO

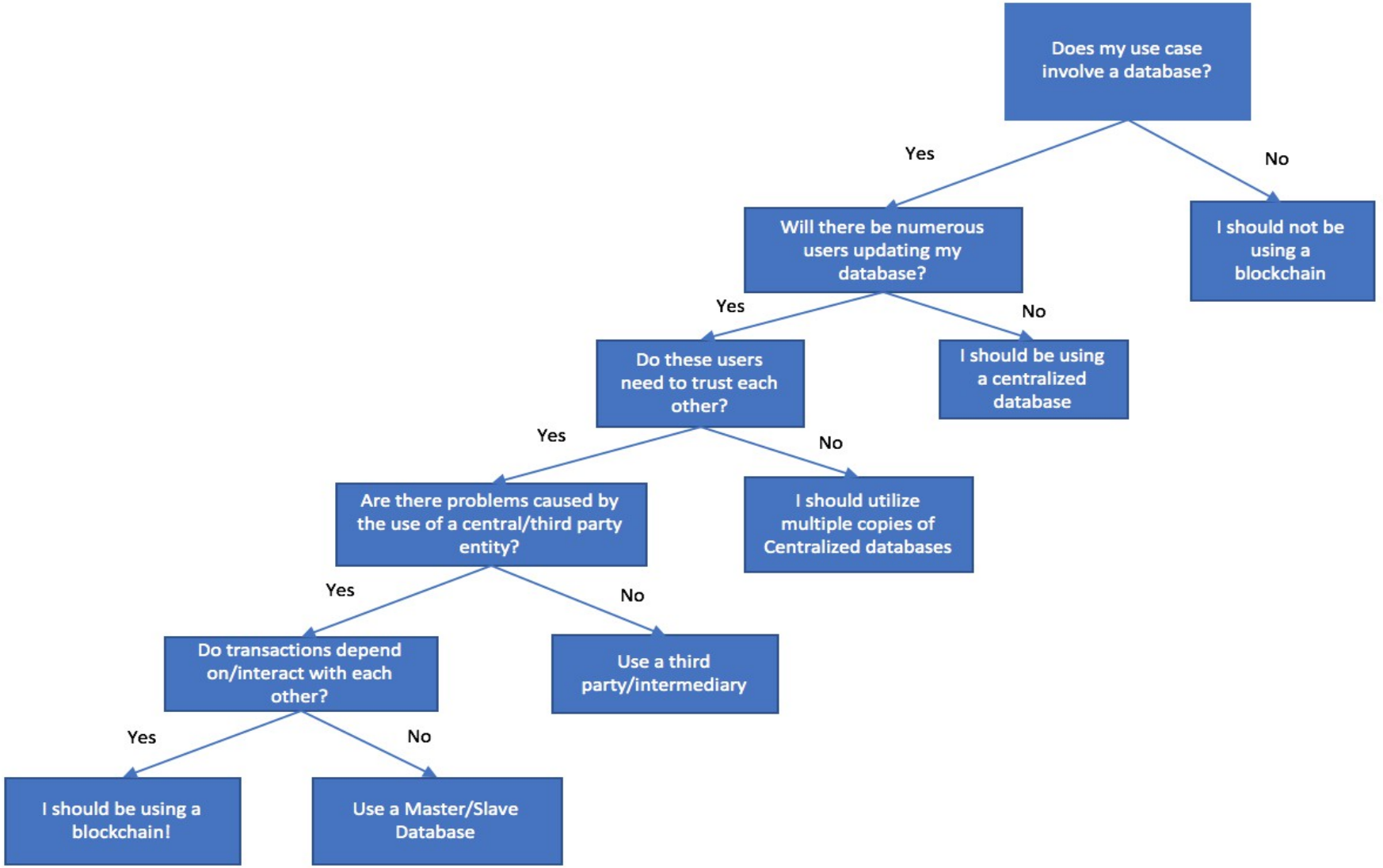
To the DAO and the Ethereum community,

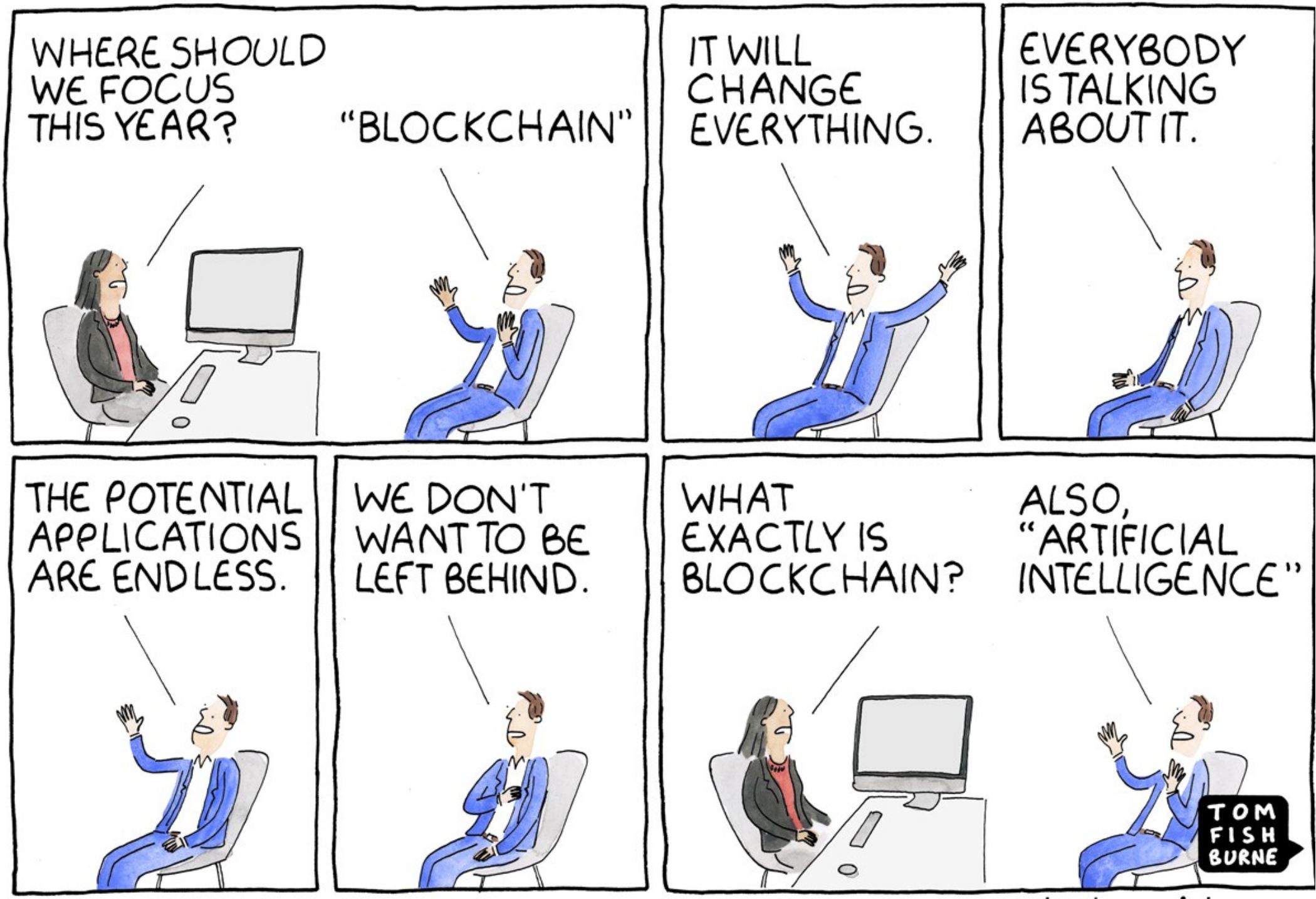
I have carefully examined the code of The DAO and decided to participate after f nding the feature where splitting is rewarded with additional ether. I have made use of this feature and have rightfully claimed 3,641,694 ether, and would like to thank the DAO for this reward. It is my understanding that the DAO code contains this feature to promote decentralization and encourage the creation of "child DAOs".

I am disappointed by those who are characterizing the use of this intentional feature as "theft". I am making use of this explicitly coded feature as per the smart contract terms and my law f rm has advised me that my action is fully compliant with United States criminal and tort law. For reference please review the terms of the DAO:

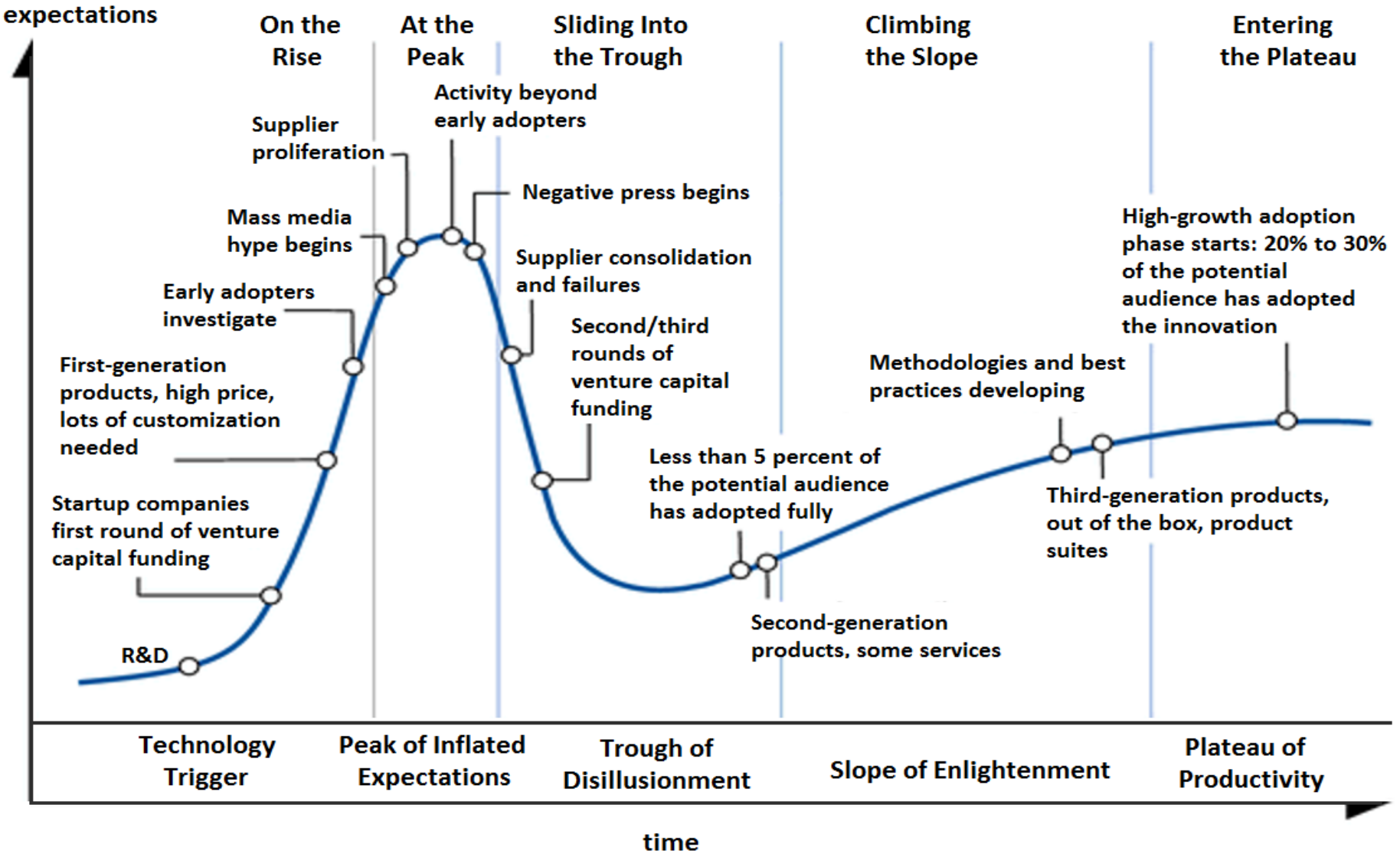
"The terms of The DAO Creation are set forth in the smart contract code existing on the Ethereum blockchain at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413. Nothing in this explanation of terms or in any other document or communication may modify or add any additional obligations or guarantees beyond those set forth in The DAO's code. Any and all explanatory terms or descriptions are merely offered for educational purposes and do not supercede or modify the express terms of The DAO's code set forth on the blockchain; to the extent you believe there to be any conf lct or discrepancy between the descriptions offered here and the functionality of The DAO's code at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413, The DAO's code controls and sets forth all terms of The DAO Creation."

Should I Use A Blockchain?




WHERE SHOULD WE FOCUS THIS YEAR?
"BLOCKCHAIN"
IT WILL CHANGE EVERYTHING.
EVERYBODY IS TALKING ABOUT IT.
THE POTENTIAL APPLICATIONS ARE ENDLESS.
WE DON'T WANT TO BE LEFT BEHIND.
WHAT EXACTLY IS BLOCKCHAIN?
ALSO, "ARTIFICIAL INTELLIGENCE"
TOM FISH BURNE

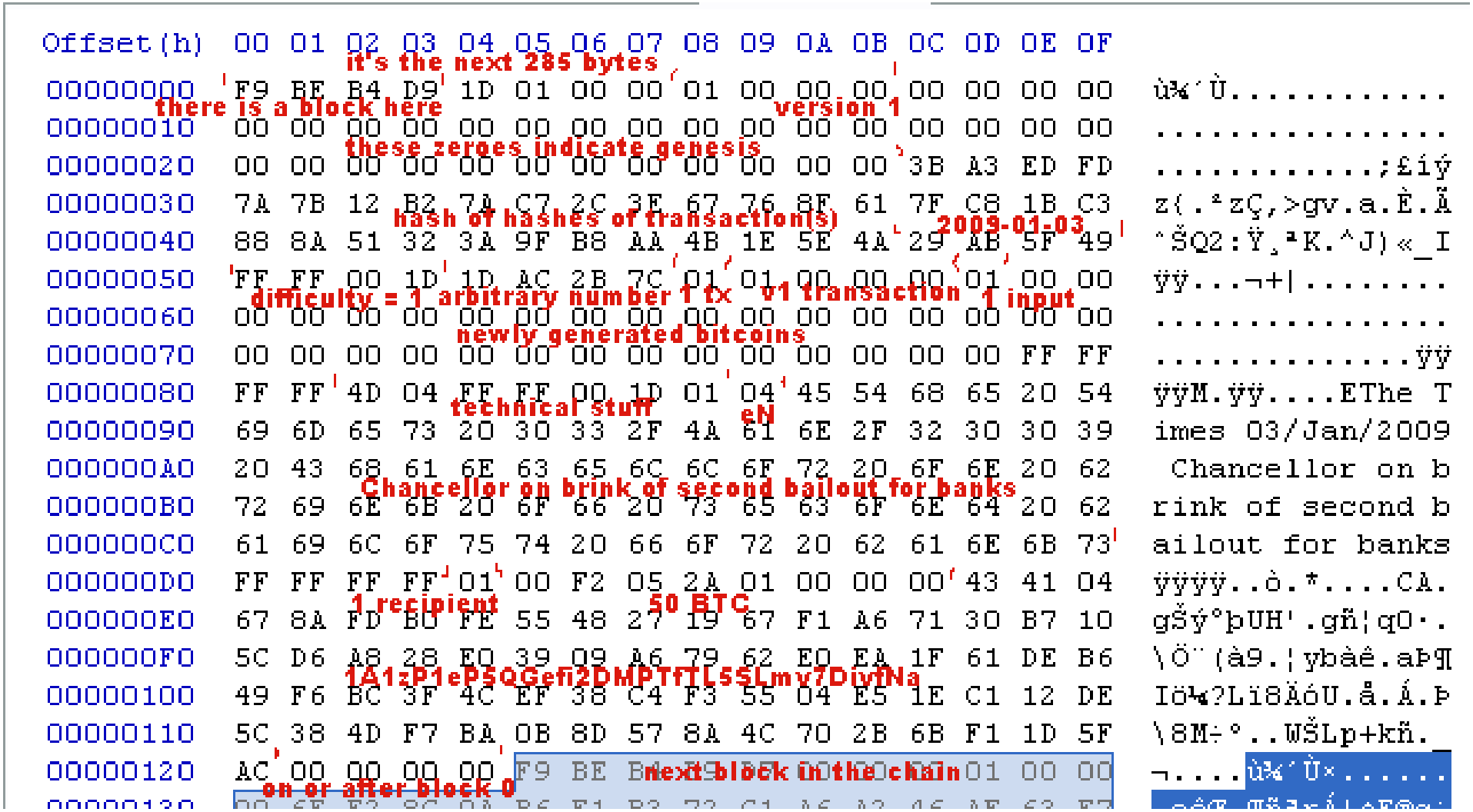
More on hype


expectations
On the Rise
At the Peak
Sliding Into the Trough
Climbing the Slope
Entering the Plateau
Activity beyond early adopters
Supplier proliferation
Negative press begins
Mass media hype begins
Supplier consolidation and failures
Early adopters investigate
Second/third rounds of venture capital funding
First-generation products, high price, lots of customization needed
Methodologies and best practices developing
High-growth adoption phase starts: 20% to 30% of the potential audience has adopted the innovation
Less than 5 percent of the potential audience has adopted fully
Startup companies first round of venture capital funding
Third-generation products, out of the box, product suites
R&D
Second-generation products, some services
Technology Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity
time

Should we use BC?

- Who writes on the DB?
- Do we really need it. LR not meeting expectations?
- Link between onchain-offchain (BC incompatibility for use as LR)

Genesis Bitcoin Message



BC LRs

- Well suited for low value assets
- Are there economic interests in making the transition? 2000 effect?
- Who's going to pay for it?
- Change the whole system to make BC fit
- Use technology as a tool or as an end?

In the absence of a central authority that controls what goes into the chain a BC based LR it is just a record of information that may or may not be true

THANK YOU

Warsaw Sept 28th 2018
Silvino Navarro
snavarro@registradores.org