

Innovativ Days

Smarter Together

Blockchain WTF ??

MAXIME LEMAIRE – TIMELAB



A person is holding a yellow sticky note in front of a computer monitor. The sticky note has the words 'BLOCK CHAIN' written in blue ink, with a blue underline under the word 'CHAIN'. The background is blurred, showing a computer screen with some colorful elements and a green light.

BLOCK
CHAIN

Qu'est-ce que c'est,
et si possible comment ça marche ?



imation

2HD IBM

formatted formatted

1.44MB

imation

12/11/03

XXX



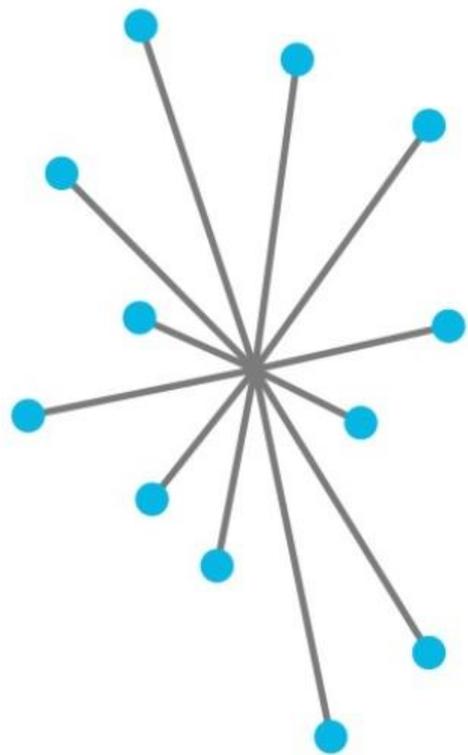
Tamper
Evidence



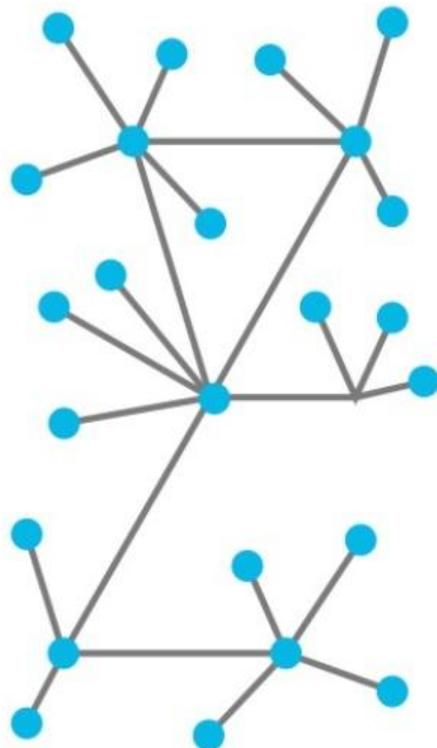
Decentralization



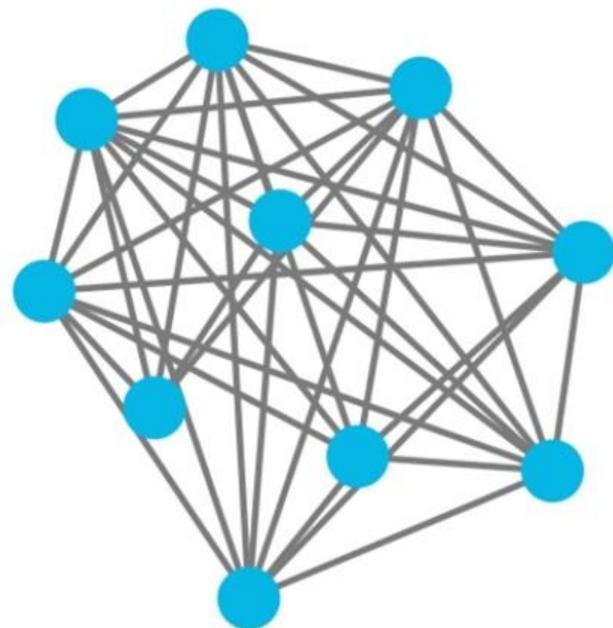
Transparency



Centralized



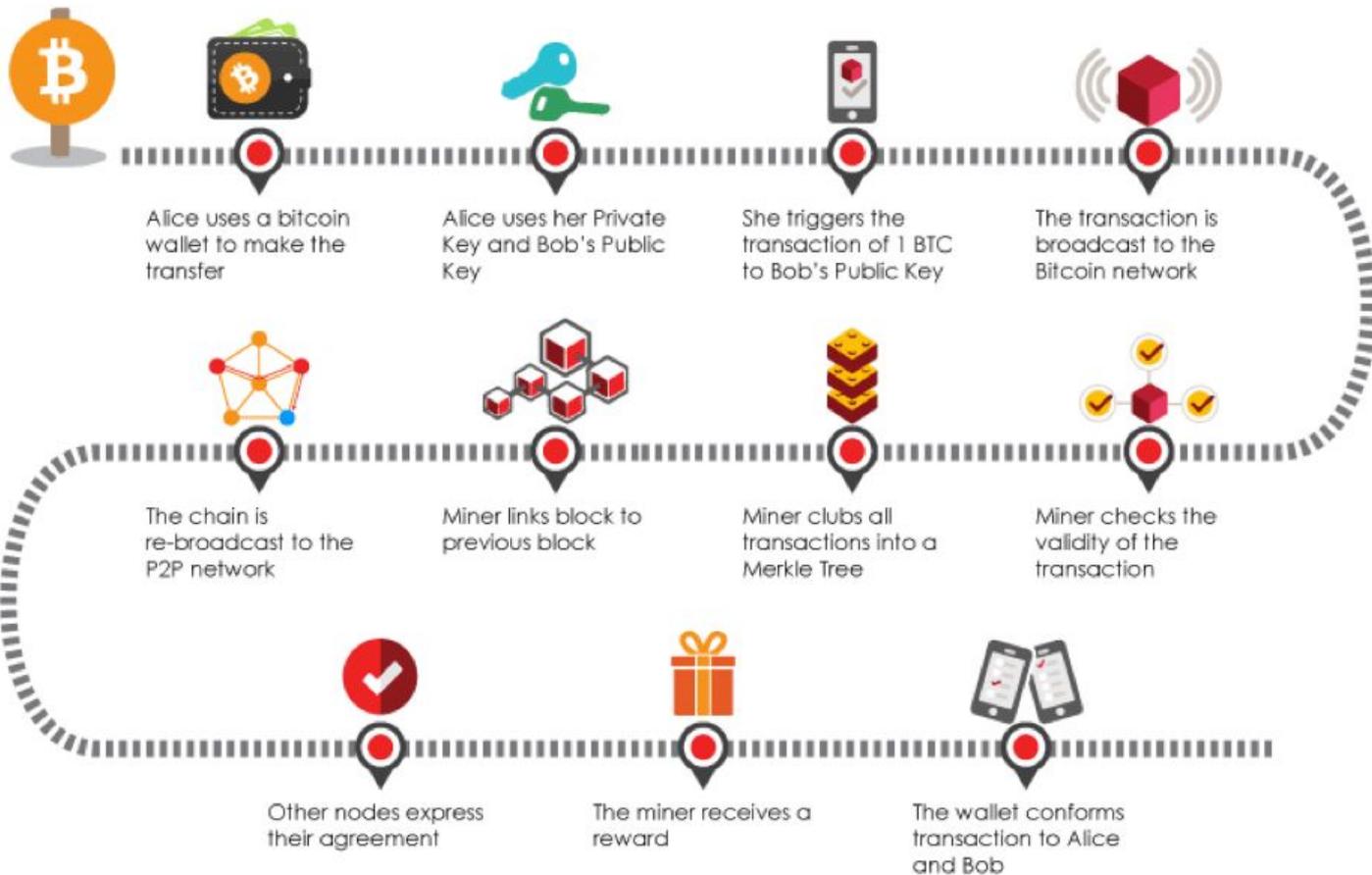
Decentralized



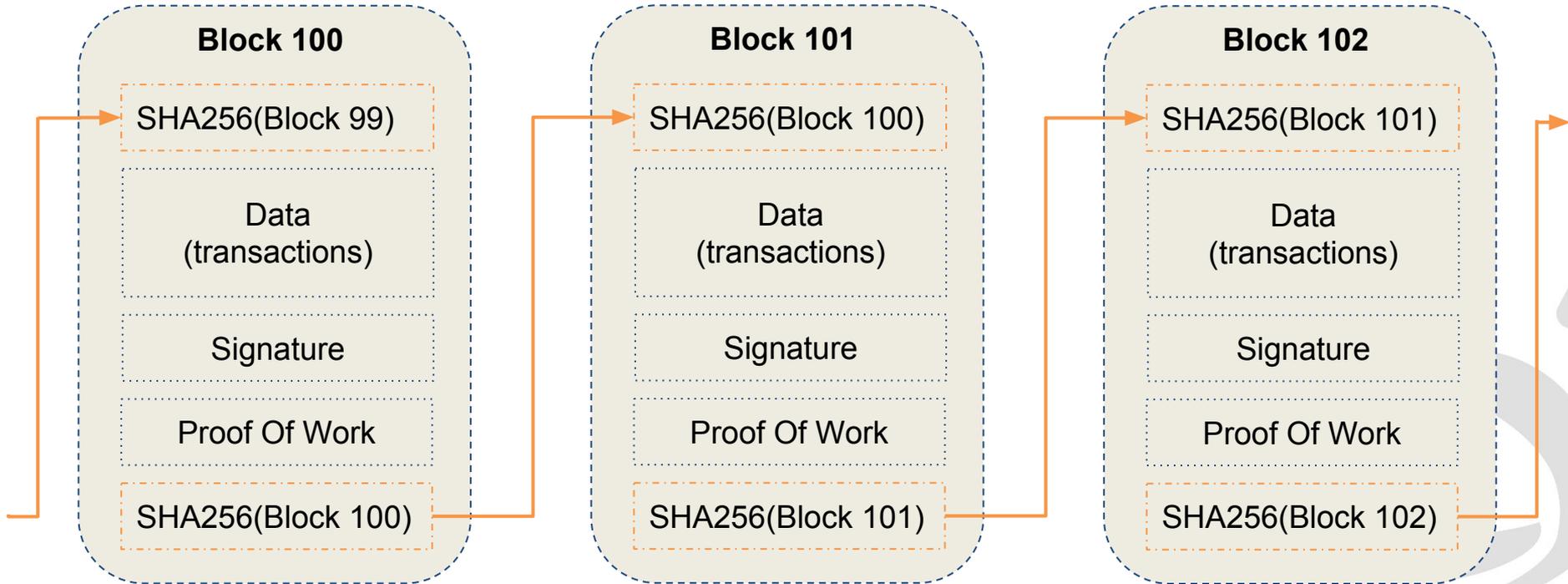
Distributed



Bitcoin



Aperçu des blocs

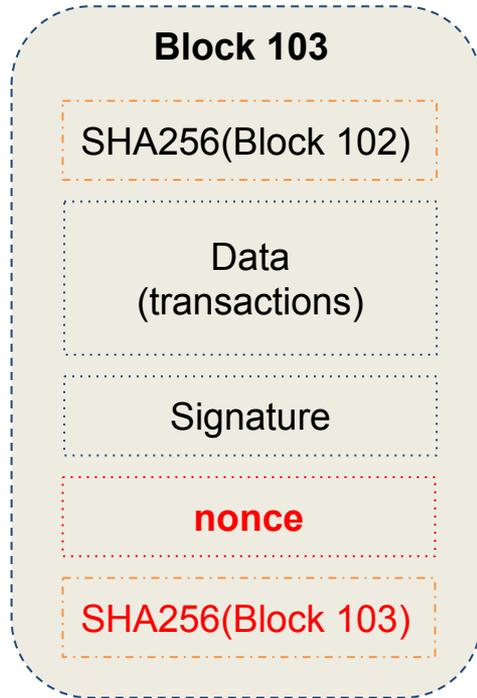


Proof Of Work

La preuve de travail est le mécanisme permettant à la blockchain Bitcoin d'obtenir le consensus

*certaines blockchains utilisent d'autres algos
exemple : Proof of Stake, Proof of Authority*

Proof Of Work



Pour qu'un bloc soit valide, son hash doit être inférieur ou égal à une valeur cible (*target*) partagée par le réseau.

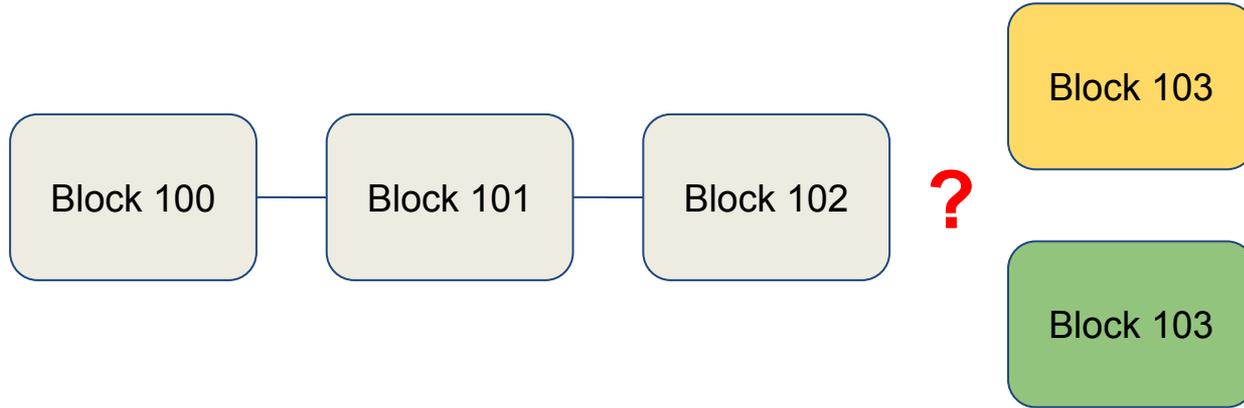
On ajoute donc au bloc un nombre aléatoire appelé *nonce* pour faire varier son hash et respecter la *target*.

Tant que le hash n'est pas valide, on recommence en modifiant le *nonce*. C'est ce qu'on appelle le *minage*.

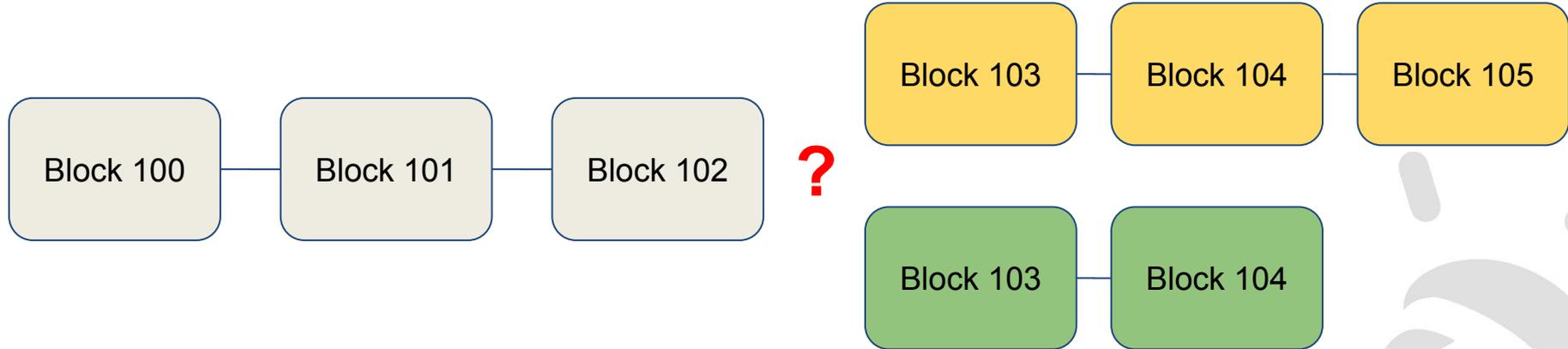
Le premier mineur a trouvé un hash valide est récompensé.

La *target* est réévaluée automatiquement tous les 2016 blocs pour ajuster la difficulté à puissance de calcul du réseau et produire en moyenne un bloc toutes les 10 minutes.

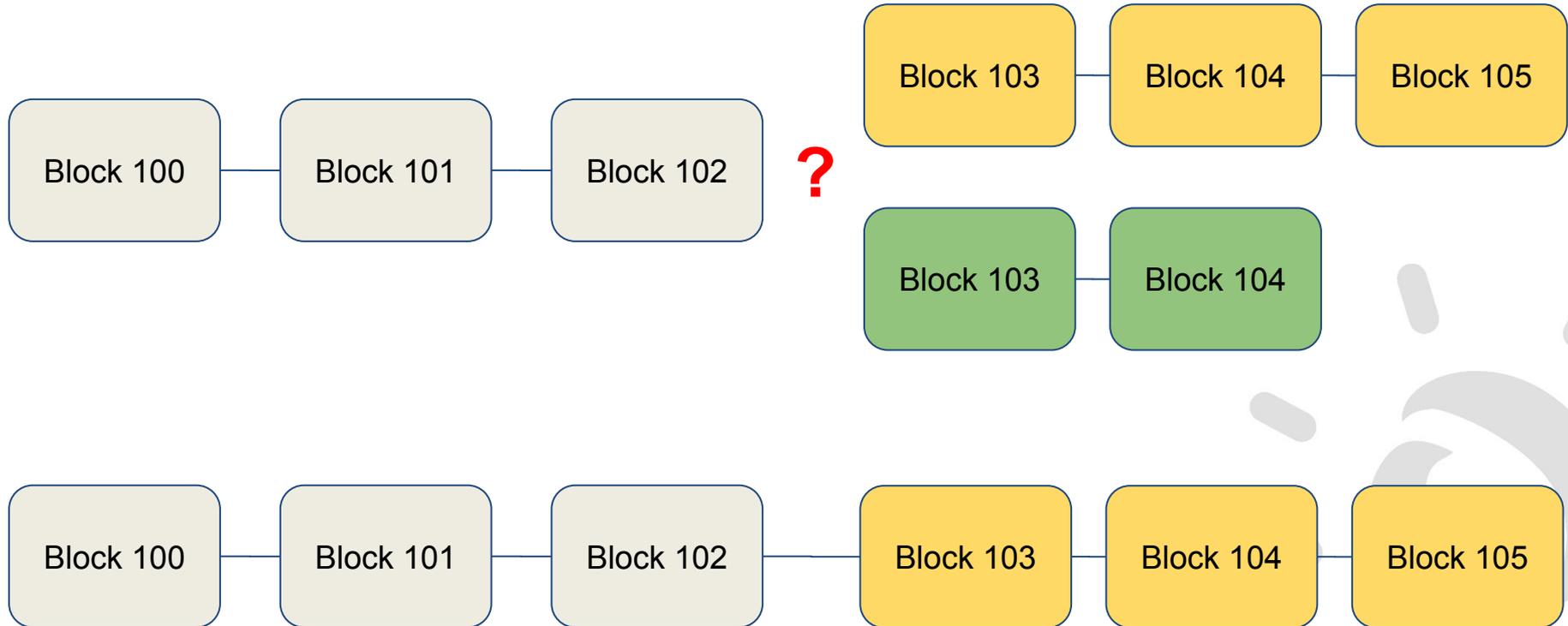
Et si deux blocs sont validés en même temps ?



Et si deux blocs sont validés en même temps ?

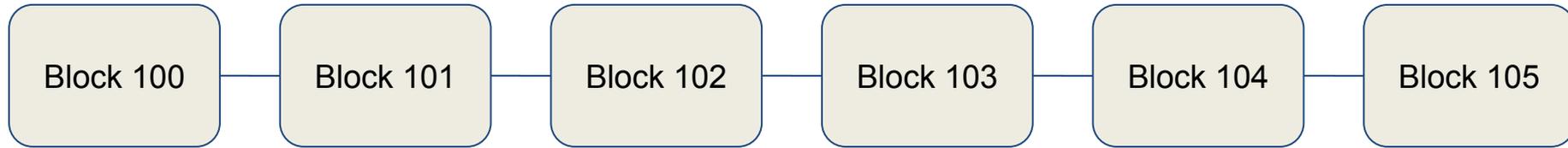


On garde toujours la chaîne la plus longue

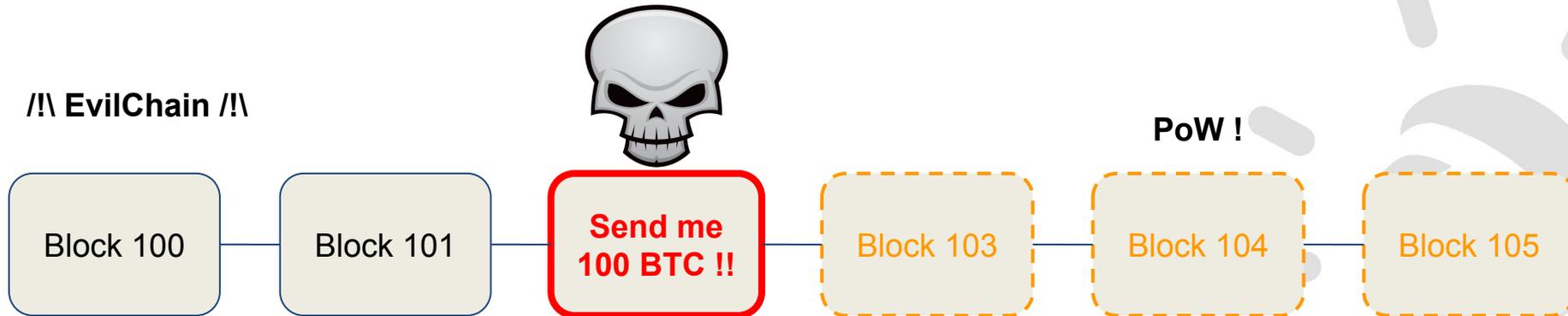


Et la sécurité ?

Valid chain..



/!\ EvilChain /\!



BLOCKCHAIN PROJECT ECOSYSTEM

CURRENCIES

BASE LAYER PROTOCOLS

- Bitcoin
- decred
- nem
- Deum
- NXT GENERATION OF CRYPTOCURRENCY
- litecoin

PAYMENTS

- STELLAR
- ripple
- metal
- Interledger
- PRIVACY
- MONERO
- VERGE
- JASH
- CASH
- CoinJoin

DEVELOPER TOOLS

SMART CONTRACTS

- EOS
- Lisk
- ethereum
- NEO
- RSK
- BOScoin

SCALING

- TrueBit
- RAIDEN

LIGHTNING NETWORK

- PLASMA

ORACLES

- oracize

SECURITY

- ZEPPELIN
- GLADIUS

LEGAL

- CODELEGIT
- AGRELLO
- COOLQIP

INTEROPERABILITY

- Polkadot
- COSMOS
- BTC RELAY
- AION
- OpenZeppelin
- Simple Token

PRIVACY

- NUCYPHER
- ROCKCHAIN

DAGs

- IOTA
- Byteball

SOVEREIGNTY

USER-CONTROLLED

- INTERNET BLOCKSTACK
- urbit
- Fabric
- HydroShare

GOVERNANCE

- ARAGON
- COLONY
- decred
- BACKFEED
- BoardRoom

VPN

- mysterium network
- PRIVATIX

COMMUNICATION

- Mercury Protocol

IDENTITY

- Toshi
- KIN
- civic
- evernym
- uport
- TrustStamp
- SHO.COM
- CRYPTID

SECURITY

- rivetz

STABLECOINS

- NuBits
- STABL
- digix
- Basecoin

FINTECH

TRADING/DEX

- 8x
- omise
- Bancor
- airswap
- dy/dx
- Counterparty
- BitShares
- EverMarkets
- BitEX
- lyber network
- EtherDelta

INSURANCE

- INSUREX
- ai gang
- ChainThat
- ETHERISC

LENDING

- SALT
- MICRO MONEY
- ripio
- charma
- WeTrust

FUNDS/INVESTMENT MANAGEMENT

- ETHlend
- NUMERA
- BLOCKCHAIN CAPITAL

VALUE EXCHANGE

CONTENT MONETIZATION

- Streamium
- g
- CIVIL
- YOUUPS
- synereo
- STEEM

FILE STORAGE

- Filecoin
- STORJ
- sia
- swarm
- MaidSafe

COMPUTATION

- golem
- RNDR
- iexec
- elastic

MESH NETWORKING

- Althea
- RightMesh

ENERGY

- Singularity
- POWER LEDGER

VIDEO

- GRID
- LIVEPEER

NON-FUNGIBLE

- enigma
- OpenMined
- datum
- streamr
- Synapse
- marketplaces
- Ethlance
- district0x
- Canva
- porrid
- CyberMiles
- OpenBazaar
- SYSCOIN
- SOCIAL
- steemit
- KIN
- PROPS by YouKnow
- Mastodon
- AKASHA

SHARED DATA

INTERNET OF THINGS

- FOAM
- IOTA
- OAKEN INNOVATIONS
- SIKORKA

SUPPLY CHAIN/LOGISTICS

- T-MINING
- Kouvola Innovation
- Sweetbridge
- MONIX
- origintrail

ATTRIBUTION

- UJO
- poet
- JAAK
- MYCELIA
- POEX.IO

REPUTATION

- ink
- bitconnect
- Bloom
- monetha

CONTENT CURATION

- userfeeds
- CURATION MARKETS

AUTHENTICITY

DATA

- FACTOM
- TIERION

TICKETING

- GUTS
- eventus
- BT BLOCKTX
- TicketChain

OTHER

PREDICT MARKETS

- GNOSIS
- VIRTUAL R
- Decentral
- STAKING
- 1 protocol
- ROCKET

GAMBL

- EDGEL
- ETHER

GAMING ESPOR

- FIRST
- ENJIN
- BISON
- Dmark
- SKRI
- UNIKO
- BIT
- DREAMTEAM

Les Smart Contracts

Les Smart Contracts sont des applications exécutant automatiquement des conditions définies et inscrites dans la blockchain.

Des frameworks sont apparus permettant de développer et déployer facilement des applications sur des blockchains publiques ou privées



HYPERLEDGER

Points forts



Traçabilité



Interopérabilité



Confiance



Sécurité



Prouvabilité

Use Cases

Greenstream

Greenstream is a blockchain disruptor focused on increasing efficiency and record keeping in the emerging Canadian legal cannabis industry.

Bitmatrix Inc.

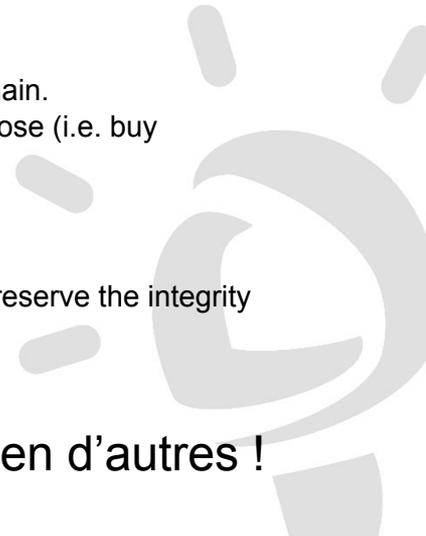
Blockchain game platform service. Gamers can own and trade their virtual assets

AID Tech

An identity/donation platform for transparent and traceable charity and remittances through the use of Blockchain. Transparent and traceable charity, as well as peace of mind that the funds will be used for their intended purpose (i.e. buy groceries or utilities, rather than alcohol, etc.)

AGETIC

Digital documents from Bolivian citizens are hashed and stored along other information in the Blockchain to preserve the integrity and creation time of public documents.

A large, faint, light grey version of the Innovativ Days logo is visible in the bottom right corner of the slide.

Et bien d'autres !

The background is a vibrant teal color with a dense field of multi-colored confetti (pink, orange, blue, yellow) scattered throughout. The logo 'timelab' is centered in white, with the 'i' and 'l' connected by a white ECG line.

timelab

Merci !



Hey !