

- 2008
- Oct
- 2011
- Apr
- Aug
- Sep
- Oct
- 2012
- Jan
- Feb
- Jun
- Jul
- Aug
- Oct
- Nov
- 2013
- Mar
- Apr
- May
- Jun
- Jul
- Aug
- Sep
- Oct
- Nov
- Dec
- 2014
- Jan
- Feb
- Mar
- Apr
- May
- Jun
- Jul
- Aug
- Sep
- Oct
- Nov
- Dec
- 2015
- Jan
- Feb
- Aug
- Sep

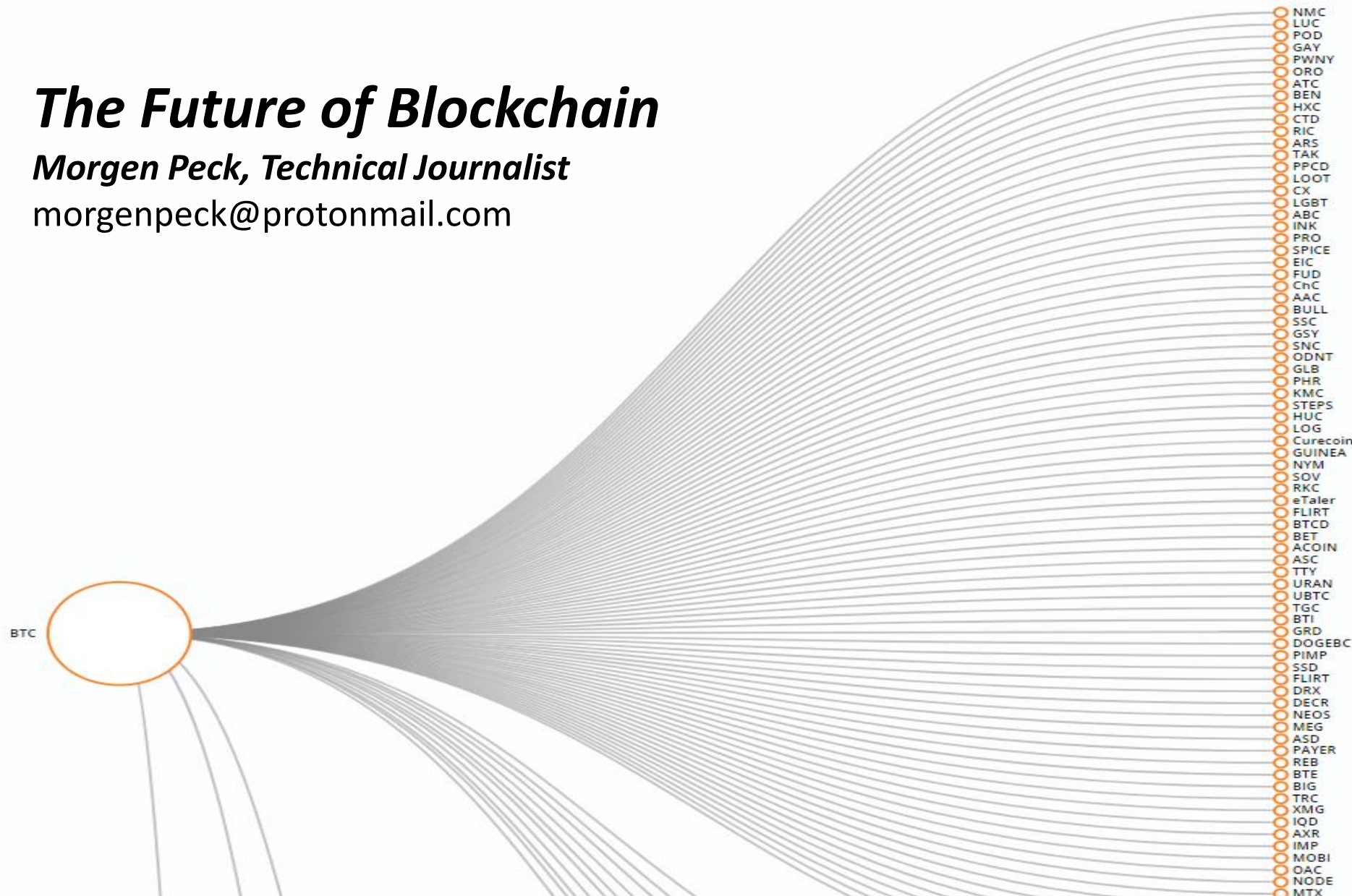
All algorithms

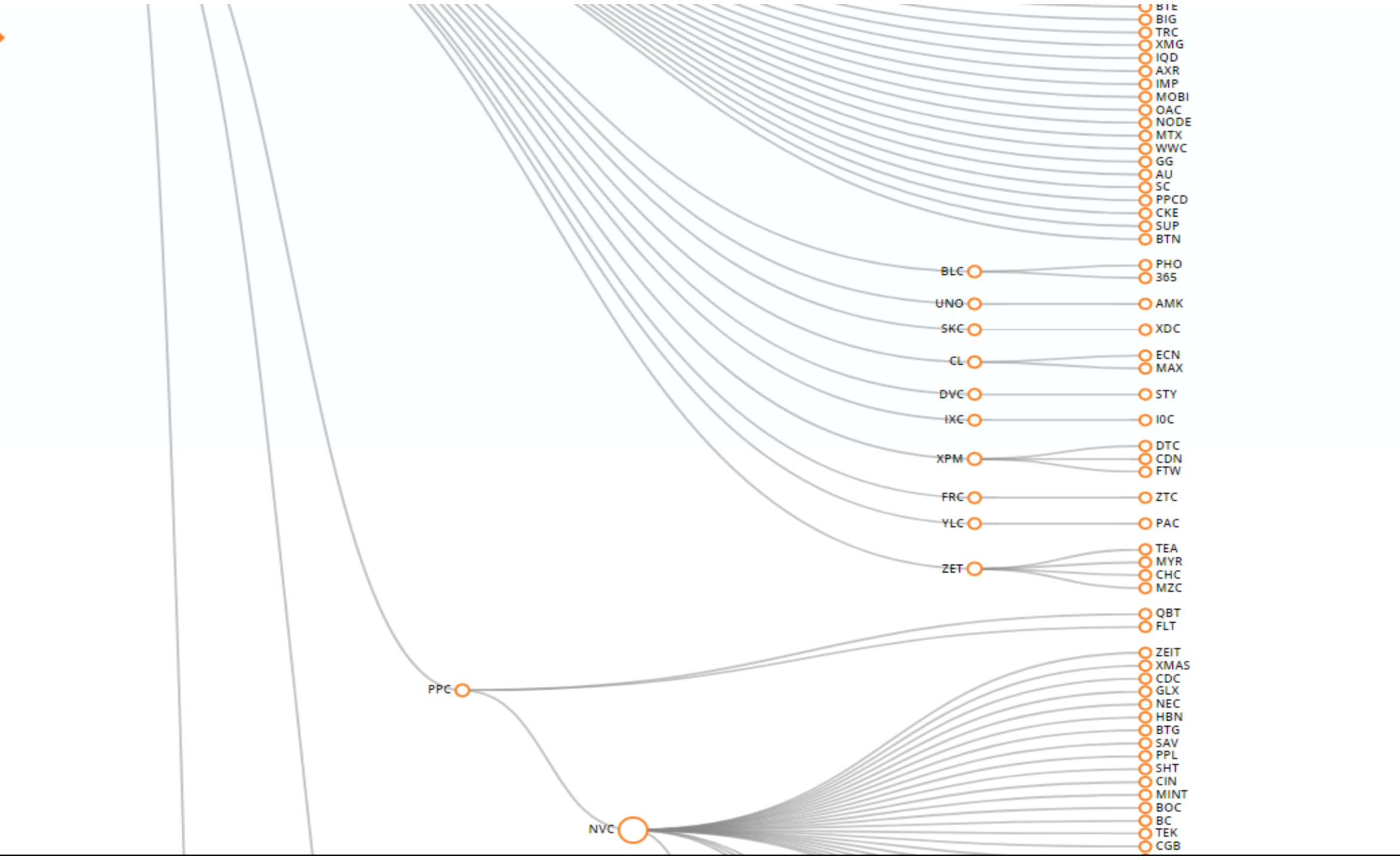
Running & defunct coins

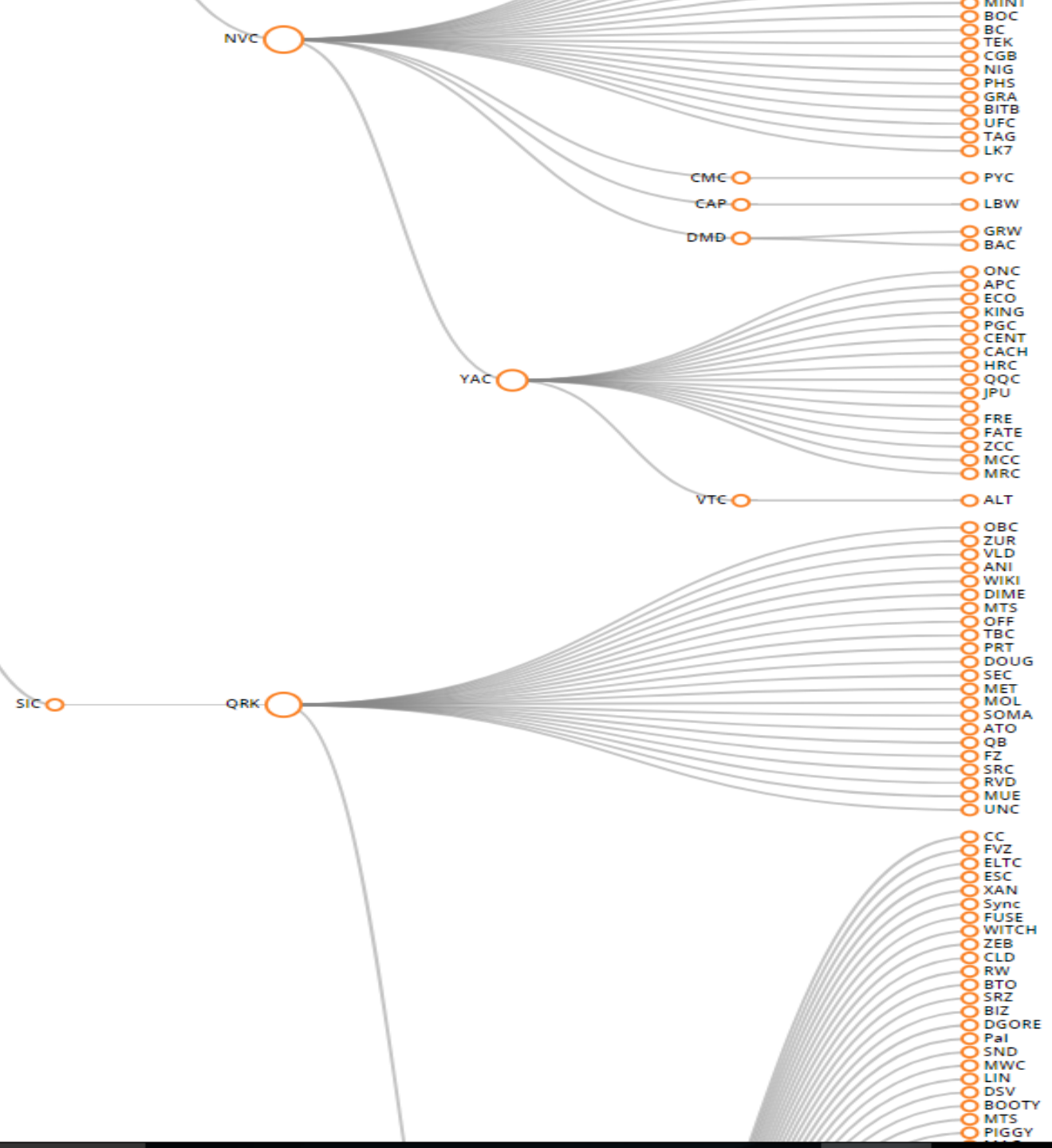
# The Future of Blockchain

Morgen Peck, Technical Journalist

morgenpeck@protonmail.com







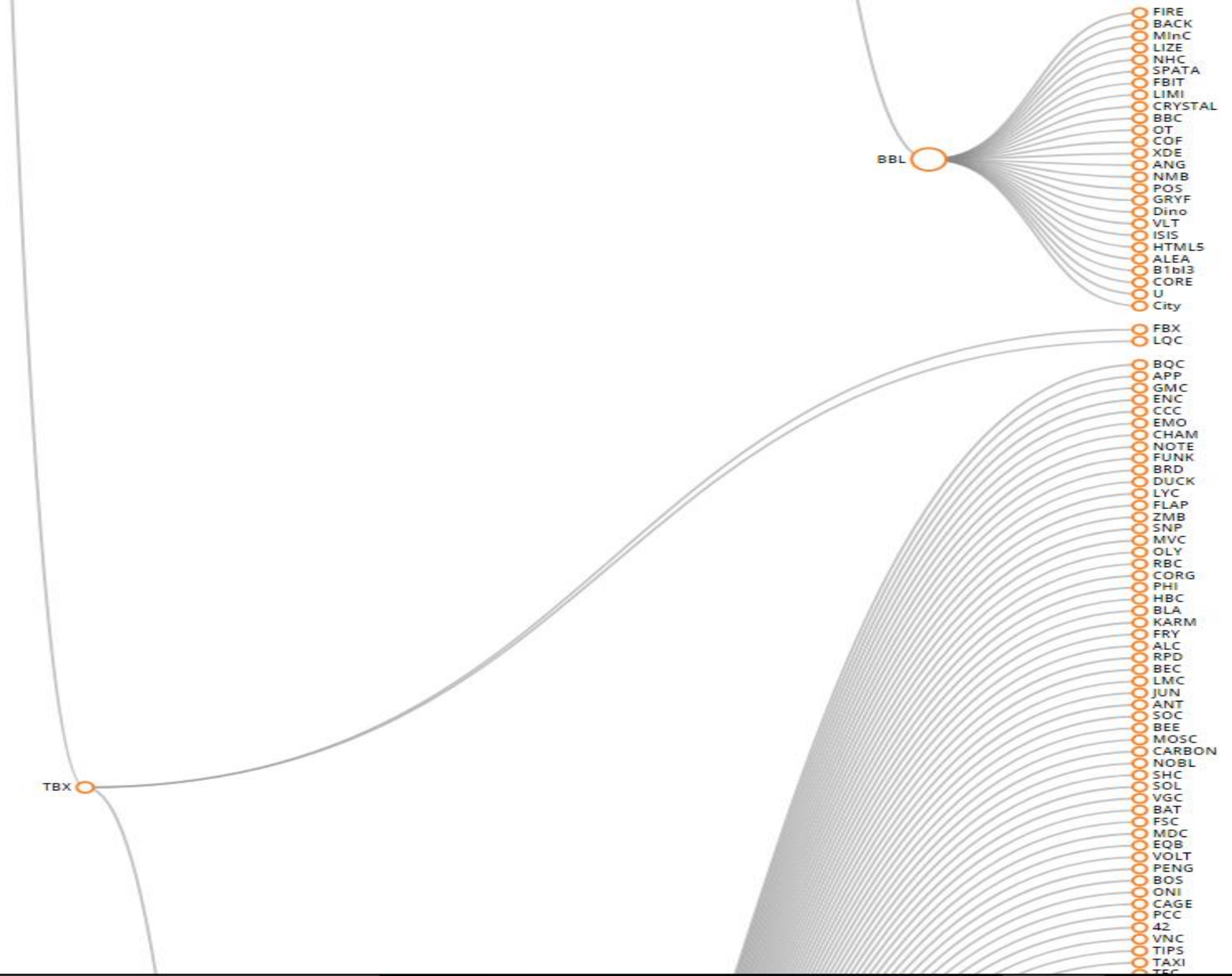
DRK



x14

- MTS
- PIGGY
- MAG
- MIL
- VMINE
- LOL
- DEPO-GBP
- MHYC
- XCR
- CSO
- WeTk
- PP
- CYX
- TRUST
- TMC
- BULBA
- RACE
- SPCC
- AZC
- HODOR
- AMBER
- GOD
- LMR
- NeWO
- CryptoXTC
- gue
- XURO
- WVS
- GLY
- FRAC
- MWC
- LIT
- Neos
- KiB
- EQX
- TRS
- CCB
- MIN
- TNZ
- WCC
- CRCK
- GRE
- CHILD
- LIMX
- ROS
- Voot
- STC
- BS
- Envy
- laura
- EXCL
- LTCX
- DP
- NL
- MTC
- suc
- METAL
- HPC
- GHOST
- NAC
- WSTL
- PURE
- SPARK
- GRN
- OPTI
- KRYP
- MOB
- ACC
- NKT
- MLGB
- LFTC
- RTC
- CBR
- TEX
- SMAC
- MC
- SOLE
- BCSH
- FIRE
- BACK





TBX

BBL

- FIRE
- BACK
- MinC
- LIZE
- NHC
- SPATA
- FBIT
- LIM1
- CRYSTAL
- BBC
- OT
- COF
- XDE
- ANG
- NMB
- POS
- GRYP
- Dino
- VLT
- ISIS
- HTML5
- ALEA
- B1b13
- CORE
- U
- City
- FBX
- LQC
- BQC
- APP
- GMC
- ENC
- CCC
- EMO
- CHAM
- NOTE
- FUNK
- BRD
- DUCK
- LYC
- FLAP
- ZMB
- SNP
- MVC
- OLY
- RBC
- CORG
- PHI
- HBC
- BLA
- KARM
- FRY
- ALC
- RPD
- BEC
- LMC
- JUN
- ANT
- SOC
- BEE
- MOSC
- CARBON
- NOBL
- SHC
- SOL
- VGC
- BAT
- FSC
- MDC
- EQB
- VOLT
- PENG
- BOS
- ONI
- CAGE
- PCC
- 42
- VNC
- TIPS
- TAXI
- TEC

LTC



- VNC
- TIPS
- TAXI
- TFC
- BLL
- MOON
- MCR
- VWC
- MRS
- HAM
- LTB
- NWC
- XXL
- HTC
- SDM
- MEOW
- PAND
- CHI
- RDD
- LDC
- YACC
- XIV
- PRC
- LOTTO
- SUN
- EUC
- SOCHI
- LOVE
- ZED
- BOS
- TOP
- AMC
- AUR
- CYB
- BELI
- POK
- BELA
- BEST
- COIN
- VAG
- PIG
- QWC
- CCN
- FLS
- SVC
- KIMO
- EXE
- GME
- JNY
- DBL
- GAM
- CRC
- ISR
- ARC
- YOLO
- TYC
- FREB
- WEC
- MXT
- PCN
- IDC
- GIL
- FUN
- ITC
- AIM
- EXC
- WFC
- PLT
- CFN
- BEL
- G8
- ZEU
- XXX
- ELC
- QTL
- HYC
- FJC
- ICE
- AID
- EZC
- MJ
- CNC
- numc
- JPC
- RC



CNC  
numc  
JPC  
RC  
CTC  
CZC  
NRB  
Kool  
RUP  
RSC  
PXC  
LTCD  
GLD  
CPTL  
FEC  
BMY  
USC  
LNKC  
QTC  
BLP  
ELP  
EVC  
EGC  
GB  
RED  
SYS  
CSC  
BUY  
LEL  
ROOT  
VLC  
TRDR  
TDC  
MANA  
NC  
SHADE  
SXC  
XBOT  
EMD  
CGA  
eDC  
BTLS  
REC  
VAC  
RCH  
SLK  
6CN  
DOLLAR  
GLC  
SNG  
MEM  
DPC  
FST  
MTLMC  
KGC  
SEED  
PWC  
SMBR  
ARG  
C2  
ALF  
ONE  
NBL  
DBU  
GIAR  
VTR  
DGC  
INS  
FOF  
DIBS  
NLG  
DGMS  
FLO  
FSC2  
XNC  
DIGI  
IFC  
CARSI  
ANC  
XTR  
FRK  
EMC2  
NET

*In the beginning, there was Bitcoin...*



# What we know about the origins of Bitcoin

- It was written by some mysterious, anonymous founder who went by the name of Satoshi Nakamoto.
- Nakamoto was sharing his work with a few people on a mailing list that was distinctly cypherpunk in nature
- In 2009 he shared his code with the world and created the first block in the Bitcoin blockchain.

And what else was happening in 2009...?

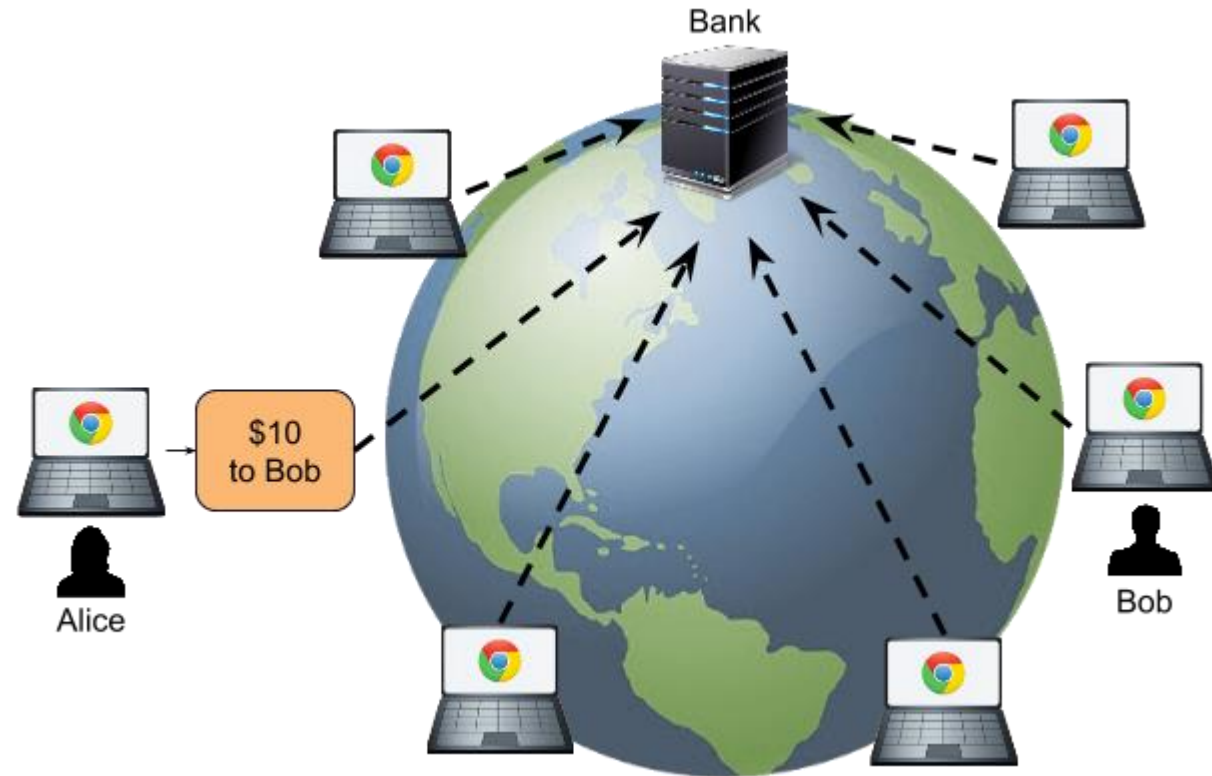


Satoshi strongly hinted at his preoccupation with the instability and inequities of the traditional financial system



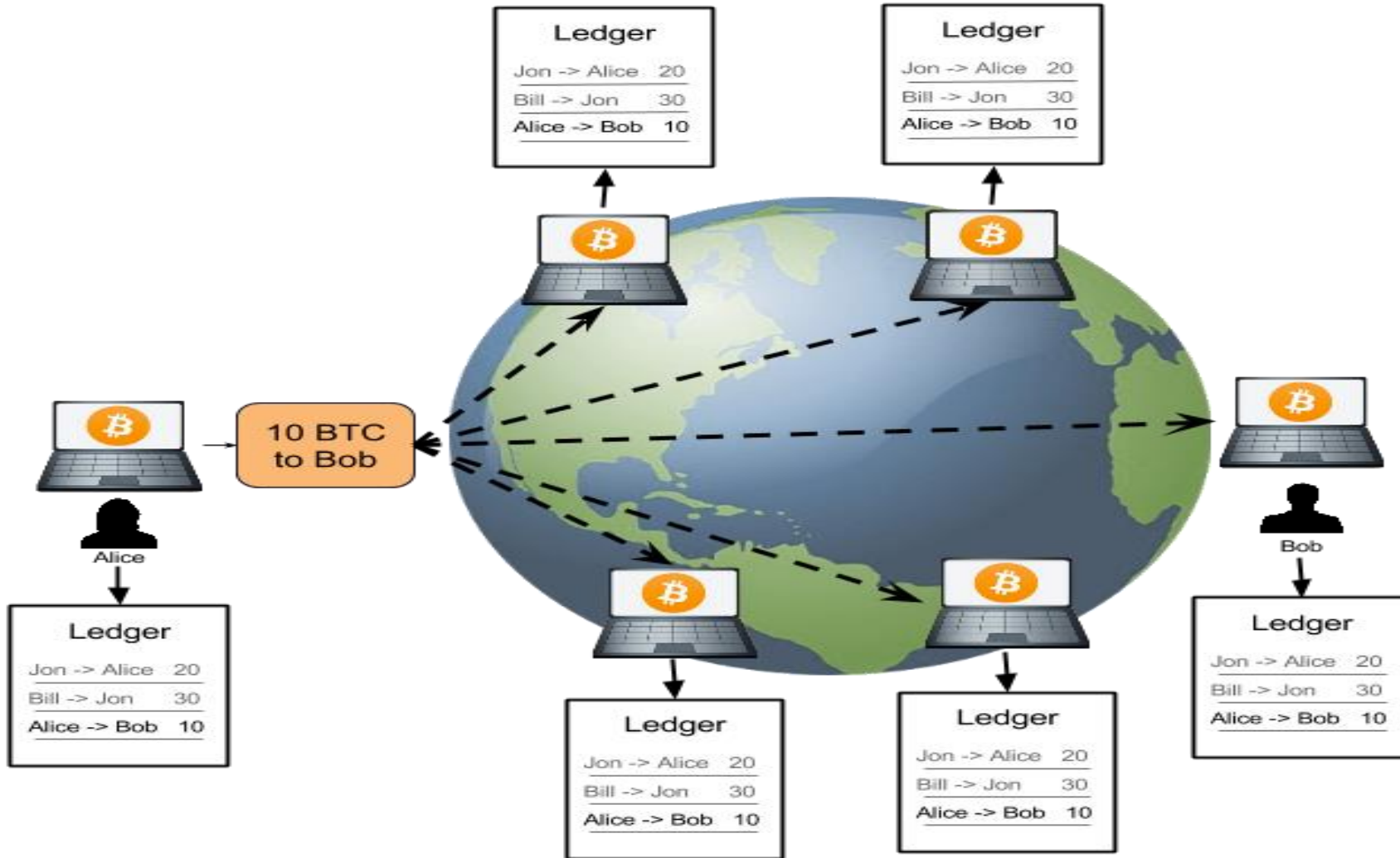
- Banks around the globe are failing.
- Governments are bailing out these institutions with taxpayer dollars without installing guarantees that their missteps will not be replicated.
- Satoshi creates a new currency that removes both banks and government entirely from the storage and transfer of value.

# This is what we're used to





# This is Bitcoin



## BITCOIN/BLOCKCHAIN

- Distributed ledger
- Strong cryptographic authentication of users
- updates executed by the public without restrictions on who can join
- money enters the economy as a subsidy to miners

# **Abstracting Bitcoin away: What is “Blockchain Technology”?**

**A blockchain is a shared data structure that grows by append only, provides authentication of users with strong cryptography, and leverages economic incentives to encourage non-trusting, unaffiliated participants to manage and secure updates**

# Early Attempts to Generalize the Technology

## The concept of “colored coins”

A “colored coin” is one that has been tagged by the user. In Bitcoin this is possible because users have the option of adding a small amount of extraneous metadata to their transactions.

By tagging transactions in Bitcoin, you can represent assets other than the native token and you can design more complex transaction structures.

“Colored coins” is smart contracts in its embryonic form.





# Enter Ethereum

In 2014, Vitalik Buterin (← that guy) announces his idea for a new platform called Ethereum

- Designed around an entirely new blockchain with its own native currency called “Ether”
- Transactions can be written with an arbitrary amount of complexity

**In Bitcoin**, miners run a specified program that checks the validity of a transaction and reassigns tokens to a new owner.

**In Ethereum**, users specify the program and then miners run it. They are free to introduce any new rules they want into the transaction



# The Horizons Expanded. The Ethos Stayed The Same

“I think a large part of the consequence is necessarily going to be disempowering some of these centralized players to some extent,” he says. “Because ultimately power is a zero sum game. And if you talk about empowering the little guy, as much as you want to couch it in flowery terminology that makes it sound fluffy and good, you are necessarily disempowering the big guy. And personally I say screw the big guy. They have enough money already.”

# Empowering the “little guy” means keeping the technology open

## **In Ethereum, as in Bitcoin:**

- Anyone can mine blocks (if they own enough hardware to compete)
- Anyone can join the network
- The code is open source

*Meanwhile...back on Wallstreet...*

- Ethereum formally launches on July 30, 2015
- In September of that year, 9 big banks join together to form R3, a consortium aimed at dragging the reluctant financial industry into the blockchain era.





# The banks are driven by a different set of needs and goals

## **NEEDS**

- Privacy for both customers and company
- Strict custody over data to satisfy regulations


## **GOALS**

- Basically make the things they already do more efficient

Banks began to question one of the fundamental features of a blockchain. It's openness.

The result is something called a "Permissioned Ledger." Or "Private Blockchain." Or "Distributed Ledger Technology." ...OY

**A blockchain is a shared data structure that grows by append only, provides authentication of users with strong cryptography, and leverages economic incentives to encourage non-trusting, unaffiliated participants to manage and secure the network.**



Today we have:

- Corda – R3
- Quorum – J.P. Morgan

Both are permissioned ledgers

## Other industries share the same concerns for custody and privacy of data

- Healthcare
- Insurance
- Voting

## Products and Industry partnerships addressing the appetite for closed blockchains

- Hyperledger
- R3
- Microsoft, IBM
- Enterprise Ethereum Alliance
- ICOs.....



# Challenges for an organization that wants to spearhead collaboration

- This is an industry that was born out of crisis and a vehement rejection of centralized control.
- It emerged from a culture that is historically suspicious of formal governance
- Tribes have already formed around technological and ideological differences
- Once formed, tribes in this ecosystem are reinforced by the prospect of getting rich

It may not be in their nature  
But they need it!

It now seems likely that we are going to be living in a multi-blockchain future. Those chains will need to be interoperable.

Thanks. Feel free to get in touch.

[morgenpeck@protonmail.com](mailto:morgenpeck@protonmail.com)