Blockchain & Cryptocurrencies Exercises

Jean Yves ZIE

2022

Exercise 1 Classical Cryptography Permutation

Decrypt this cyphertext : IYLE SZES MUBR LLEA QBUO ENVN OEUV SOSI OE

Exercise 2 Classical Cryptography Caesar

Decrypt this cyphertext (find key= ?).
You can use `https://www.dcode.fr/chiffre-cesar`
“ X’zno...
Npkzmxvgdamvbdgdnodxzskdvgdyjxdjpn
X’zno qmvd lpz xz hjo omjk gjib zno kvmavdozhzio vomjxz
Hvdn avpo gz ydmz zo qjpn nzmzu v gv kvbz zo kgpn kmzxjxz
Npkzmxvgdamvbdgdnodxzskdvgdyjxdjpn
Ph ydyygz ydyygz ydyygz ph ydyygz vt
Ph ydyygz ydyygz ydyygz ph ydyygz vt”

Exercise 3 Classical Cryptography Caesar

Decrypt this cyphertext (find key= ?). Which book is that from ?
You can use `https://www.dcode.fr/chiffre-cesar`.
“ Cpijjgaxyz odj ttc lxaatztjgxvt kddgqxyvpcvtg vttc ktghrwxa oxtc ijhhtc bxyc txvtc gdds tc yjaaxt. Bppg idrw xh oxy, oxy paattc, ktta qtapcvgxyztg spc yjaaxt paatc, dbspi xz wppg lpitg wtq vtvtktc, tc wppg dcstg ttc hidae wtq vtoti ; dbspi xz wppg wtq qthrwji bti ttc zpbtghrwtgb tc st gjehtc kddg wppg wtq vtsdds (qtwpakt ttc tcztat wxtg tc sppg, kddg st kaxcstgh) ; dbspi xz wppg zaprwitc tc wppg vthcdtu tc otauh wppg olxyvtc wtq ppcvtwddgs ; dbspi oxy bxyc gddh xh. Tc wxy vxcv itgjv cppg st kdh. ”

Exercise 4 Classical Cryptography Vigenère

You can use `https://www.dcode.fr/chiffre-vigenere`.
Find the key of this ciphertext :
“Nl gwaaxticeujti jue ysg oix ftwhkapnppw ig we htjtyqwslkp w’fveehjlry c avtvpkjt oix opwxcrix (cdwztlry ezrkkoisvteqkei, fweljpemhkei jv trygrvnvp) is u’lmicyx xqfzjpe hj upgwgew tw npju. Ppqg di ikdxnpryj fp pf ueilcysltltmkp uzk qenv aexupv npltjtny zp xixulkj flrx wy ezvci rgdwfip eqqcw vwp pf eccuvzkwcalng cisf fr rgdwfip wzrasxgxisv trnpeiqntkndwi f cfxwg byj sfm-ig-ovtke.”

Exercise 5 Classical Cryptography Vigenère

You can use `https://www.dcode.fr/chiffre-vigenere`.
Find where this quote is from : “yrknylw, rngg ko jaxo rw zrh tebke zkdiiafnmw ea.”

Hint : Bruteforce the key length until the message seems to make some sense

Exercise 6 Cryptography quiz

1. Alice wants to encrypt a message for Bob. She uses
   (a) Bob's public key
   (b) Bob's private key
   (c) her public key
   (d) her private key
2. Alice wants to decrypt a message received from Bob. She uses
   (a) Bob's public key
   (b) Bob's private key
   (c) her public key
   (d) her private key
3. Alice wants to sign a message. She uses
   (a) Bob's public key
   (b) Bob's private key
   (c) her public key
   (d) her private key
4. Bob needs to verify the previous signature. He uses :
   (a) Alice's public key
   (b) Alice's private key
   (c) his public key
   (d) his private key

Bonus Thanks to computers, we are :
   (a) today able to decrypt all the secrets messages from Queens and Kings, all the ancient languages.
   (b) still not able to decrypt some old texts.

Exercise 7 Key exchange

Alice wants to send a box of chocolate through the mail to Bob. She does not want the chocolate to disappear because Eve is the one doing the delivery. Alice has a lock with a key. Bob has a different lock and the corresponding key.

1. How do they proceed ?

Exercise 8 Hack me if you can

You want to see the content of the admin's phone, David. What you know :

- David often forget his phone at lunch break,
- He takes at least an hour of break,
- He is a big fan of tennis
- that his code is most likely the score of a match won by his idol(Federer :grin :) in a 2 sets game

1. Estimate the number of trials you need to break in.
2. Should you accept this mission, if you take 30s per trial ?

Exercise 9 Cryptography quiz Private key generation

Assess(yes/no) with a quick justification, if it is secure to generate your private keys from :

1. a birth date
2. some digits of Π
3. sha256(your password)
4. throwing a dice (enough time)
5. your favourite quote

Exercise 10 Commit & Reveal

Pick a number in $[\![0;10]\!]$. I will try to guess this number. My guess is the number that when hash with SHA256 gives 7902699BE42...

1. Was my guess correct ? See an explanation here `https://www.reddit.com/r/dataisbeautiful/comments/acow6y/asking_over_8500_students_to_pick_a_random_number/`.
2. Was it possible for me t change my guess without you noticing ?
   Now I have a list of 8 messages $[\![m_1;m_8]\!]$. I want to efficiently commit them so that I don't have to reveal everything to prove to you that I didn't cheat.
3. How should I do it ?

Exercise 11

Find the word that gives the following hash :
C4E793C81EE40370D827D0CBE748D246CFFCA2CBE959383EDF0976D041ECE9E5

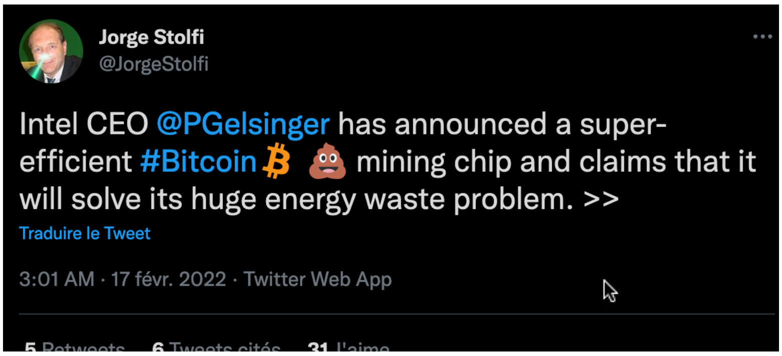
Exercise 12 Proof-Of-Work

Here we want to find a POW on the SHA256 of the string "emn" + some number, like "emn9999", that starts with 00.Ex :
SHA256(emn1)= 125e258fa4b011704fe744e1d8c28090ecf2180b2cd28a6fa55b21374df819bf
SHA256(emn2)= 5112eb13aa45d31e01557b7c7f4ba4c71c75f79300fc6aa56737998b4c5c2566
Notice that the hashes are written in hexadecimal, which use 16 characters : "0- 9" and "a-f".

1. Estimate the number of trials you would need.
2. Give the value of the SHA256 of "EMN566".
3. For the string "EMN", the first hash that works is at trial 566. This means that from "EMN1" to "EMN565", we do not get a hash starting with enough 0. Compare that with your answer from 1). Can you explain the difference ? For the questions, team work can be helpful.
4. Starting at "emn1", find a POW that starts with 00.
5. Using "INSA" + a number, find a POW that starts with 000000 or more.

Exercise 13 POW

Suppose the hash rate of Bitcoin is 100 EH/s, or 100.10^{18} H/s. Eve wants to gain enough mining power attempt a *double spending* attack.



Jorge Stolfi
@JorgeStolfi

Intel CEO @PGelsinger has announced a super-efficient #Bitcoin ₿ 💩 mining chip and claims that it will solve its huge energy waste problem. >>

Traduire le Tweet

3:01 AM · 17 févr. 2022 · Twitter Web App

5 Retweets 6 Tweets cités 31 J'aime

FIGURE 1 – Mining

1. There is 51 EH/s that are available at Nicehash, a company that let's you rent/loan your mining power. Eve rents the 51 EH/s from Nicehash. Will her attack succeed with the rented hash rate ?
2. Here instead, she goes to Bitmain, a company that builds ASICs i.e special machines that are optimised to mine Bitcoin. She orders enough ASICs to produce 51 EH/s. Will her attack be successful ?

Exercise 14 A broken proof of work (2 points)

From `https://cs251.stanford.edu/`

Let H be a hash function $H : X \times Y \to \{0, 1, ..., 2^n - 1\}$ for a proof-of-work scheme. Once an $x \in X$ and a difficulty level D are published, it should take an expected D evaluations of the hash function to find a $y \in Y$ such that $H(x, y) < 2^n/D$. Suppose that $X = Y = \{0, 1\}^m$ for some m and consider the hash function

$$H : X \times Y \to \{0, 1, ..., 2^{256} - 1\} \text{ defined as } H(x, y) := SHA256(x \oplus y)$$

Here $\oplus$ denotes a bit-wise xor. Suppose D is fixed ahead of time. Show that a clever attacker can find a solution $y \in Y$ with minimal effort once $x \in X$ is published.

Hint : the attacker will do most of the work before x is published.

Exercise 15 Ethereum address

1. Generate an Ethereum address
2. Give a proof that you own this address
3. Is it safe for you to receive funds on that address ? Why ?

Exercise 16 Bitcoin Genesis

Find the message Satoshi put in the Bitcoin Genesis block. What does this prove ?

Exercise 17 Mining (3 points)

Do you think that a super-efficient mining chip will reduce Bitcoin's energy waste (Figure 1) ? Explain your position.

Exercise 18 Ethereum Transaction

This is an Ethereum transaction :
`https://ropsten.etherscan.io/tx/0xc7b8b91fd00a6aadfeca2bc268811fade6c833786139c3c6d5352510a94e`
I made this transaction to add some data (a text) in the Ethereum blockchain.

1. Find this text.
2. Since the transaction is accepted in the ledger, this text should be kept forever. This might actually not be the case. Explain why.

Exercise 19 GDPR vs blockchain

Discussion (2,3 paragraphs maximum) : Can a blockchain-based system or service be compliant with the GDPR ?

Problem 1 Rock Paper Scissors (8 points)

We want to use a smart contract to play a decentralized version of "Rock Paper Scissors". Each player can send "Rock", "Paper" or "Scissors" to play during a round.

1. *(1pt)* Why should you not play if you have to go first ?
2. *(1pt)* You complained to the devs and they make a new version where the playing order is the alphabetical order of the addresses. Explain how to increase your chances of winning.
3. *(1pt)* The new version hashes your plays, e.g. $tx = SHA256(''Rock'')$. Explain the issues with this version.
4. *(1pt)* Improve the previous protocol with a "commit & reveal" scheme.
5. *(4pts)* Using your improved version, Alice and Bob want to play for some tokens, say 100€. Each player sends the tokens before the round, commit their play then send a reveal transaction. Once both plays are revealed, the winner can take his or her prize. Explain how the loser can stop the winner from taking his or her money. Can you make a new improved version of the protocol that fixes this ?

Problem 2 Decentralized Finance hack

In this exercise we will explore the world of DeFi(Decentralized Finance) and the services built can be used as Lego bricks. We will see the use and dangers of having protocols interacting with each other in a permissionless manner.

First let us look at flash loans. Those are special functions of a smart contract that lets you, in the same transaction, borrow a cryptoasset without any collateral, do all the operations you want with those assets with the only constraints that in the last step of the transaction, you should repay the borrow cryptoassets plus the interests. As an example we will use Aave that has a 0.09% interest on flash loan (`https://aave.com/flash-loans/`).

Note that the smart contract code guarantees that, if we don't payback the loan plus interest, there is no change to the blockchain state. So if you try to execute an arbitrage, either you succeed and use your profit to pay the interest of the flash loans, either it fails (and you only loose the transaction fees). For more details : `https://academy.binance.com/en/articles/what-are-flash-loans-in-defi`

We will also use decentralized exchange called Uniswap (`https://uniswap.org/faq/#how-does-uniswap-work`). Its particularity is that you can, at any time, trade between two cryptoassets X and Y. There is a pool of coins, x coins of X and y coins of Y such that $x * y = k$, where k is constant. So when a trade occurs, i.e you send one asset in exchange of the other, the quantities in the pool change but k stays the same. Note that the price of X in terms of Y is y/x.

Scenario : I create a token on Ethereum, called EMNCoin(EMN), and I want to do an ICO(Initial Coin Offering) where people can buy EMN with USD. I want to sell the token at 1% of Ethereum(ETH) price, which is \$500. So I am expecting to sell them at \$5 each. Since the price of ETH can move, I will use Uniswap as a price Oracle. This means that, when one wants to buy some EMN with some USD, the smart contract of EMNCoin will fetch the price of ETH from the Uniswap Pool, compute the price of EMN and send the right amount of coins.

Goal : Create a transaction with many steps that will use a flash loan to profit from the ICO. We will assume thare is another decentralized exchange(DEX), where we can sell EMN for exactly \$5. So you want to perform an arbitrage between the EMNCoin and the DEX by buying cheap and selling at a higher price. *This can be done in an Excel spreadsheet for those who want. We will use the data in the following table.*

name	description	quantity/amount
ICO	EMNCoin smart contract for the ICO	500000 EMN
POOL	Uniswap pool for the pair ETH/USD	
x	Quantity of ETH on POOL	1000 ETH
y	Quantity of USD on POOL	500000 USD
k	Constant of ETH/USD on POOL	500000000
FEE	flash loan fees on Aave	0.09%
DEX	Other DEX where we can sell EMN	

1. How much would it cost to take a \$1 billion loan ?
2. Why are flash loans not possible in traditional finance ?
3. Why can't we use a flash loan to trade on exchanges (cryptocurrencies brokers) ?
4. What simple countermeasure against flash loan can you implement in a protocol ?
5. Give the resulting $x, y, k, y/x$ on POOL after a trade to buy 100 ETH.
6. Give the resulting $x, y, k, y/x$ on POOL if instead it is a sell order of 200 ETH ?
7. What do you notice about the price of ETH/USD in POOL with the two previous transactions ?
8. Taking a flash loan of a chosen amount, perform the arbitrage to maximise your gain in this single transaction. You will detail each step you take and the changes that unfold. The grade will depend on the success or failure of the arbitrage and the profit made.
9. Why is it hard to profit from those types of financial opportunities, being an arbitrage or other, when dealing with cryptocurrencies ? *Hint* : Think about pending transactions.

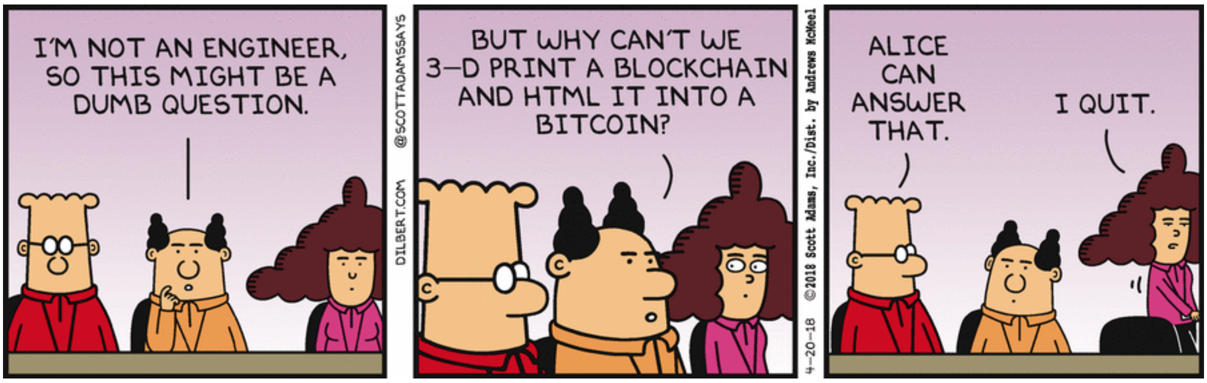

I'M NOT AN ENGINEER, SO THIS MIGHT BE A DUMB QUESTION.
BUT WHY CAN'T WE 3-D PRINT A BLOCKCHAIN AND HTML IT INTO A BITCOIN?
ALICE CAN ANSWER THAT.
I QUIT.
DILBERT.COM @SCOTTADAMSSAYS
4-20-18 ©2018 Scott Adams, Inc./Dist. by Andrews McMeel

FIGURE 2 – noob question

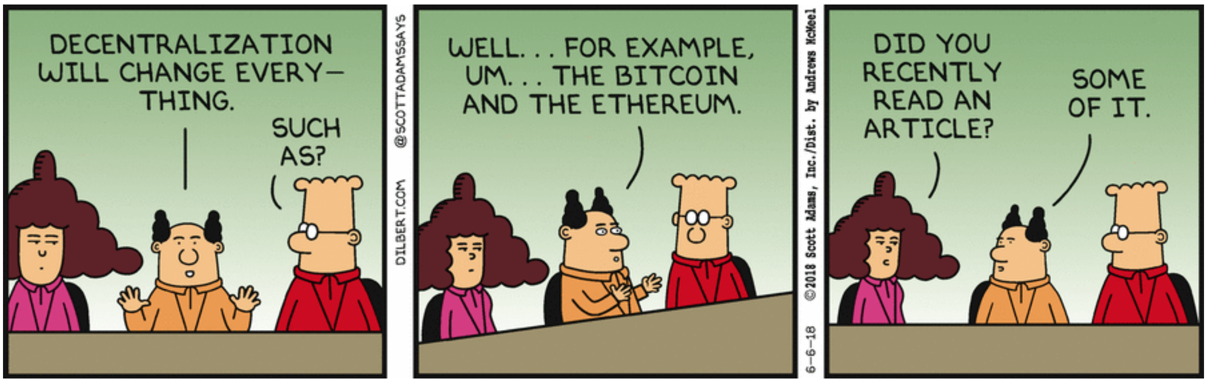

DECENTRALIZATION WILL CHANGE EVERY-THING.
SUCH AS?
WELL. . . FOR EXAMPLE, UM. . . THE BITCOIN AND THE ETHEREUM.
DID YOU RECENTLY READ AN ARTICLE?
SOME OF IT.
DILBERT.COM @SCOTTADAMSSAYS
6-6-18 ©2018 Scott Adams, Inc./Dist. by Andrews McMeel

FIGURE 3 – decentralization

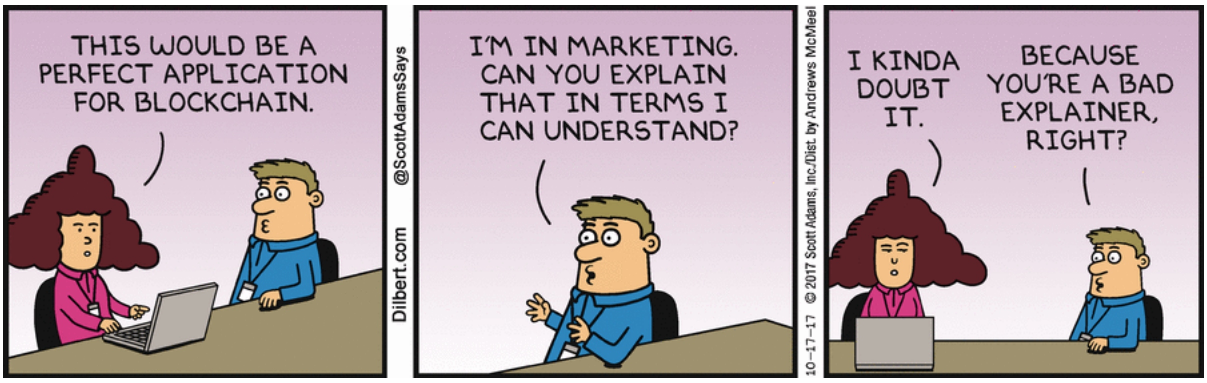

THIS WOULD BE A PERFECT APPLICATION FOR BLOCKCHAIN.
I'M IN MARKETING. CAN YOU EXPLAIN THAT IN TERMS I CAN UNDERSTAND?
I KINDA DOUBT IT.
BECAUSE YOU'RE A BAD EXPLAINER, RIGHT?
Dilbert.com @ScottAdamsSays
10-17-17 ©2017 Scott Adams, Inc./Dist. by Andrews McMeel

FIGURE 4 – explanation

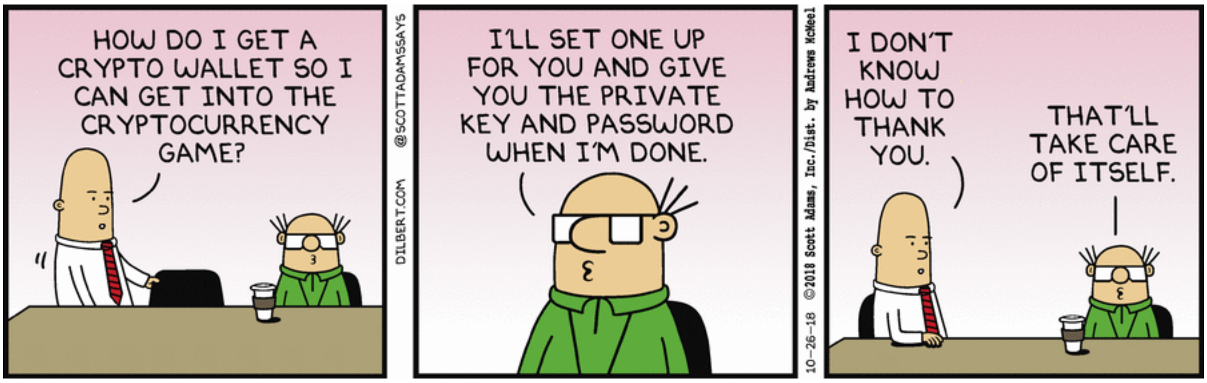

HOW DO I GET A CRYPTO WALLET SO I CAN GET INTO THE CRYPTOCURRENCY GAME?
@SCOTTADAMSSAYS
DILBERT.COM
I'LL SET ONE UP FOR YOU AND GIVE YOU THE PRIVATE KEY AND PASSWORD WHEN I'M DONE.
10-26-18 ©2018 Scott Adams, Inc./Dist. by Andrews McMeel
I DON'T KNOW HOW TO THANK YOU.
THAT'LL TAKE CARE OF ITSELF.

FIGURE 5 – private key1

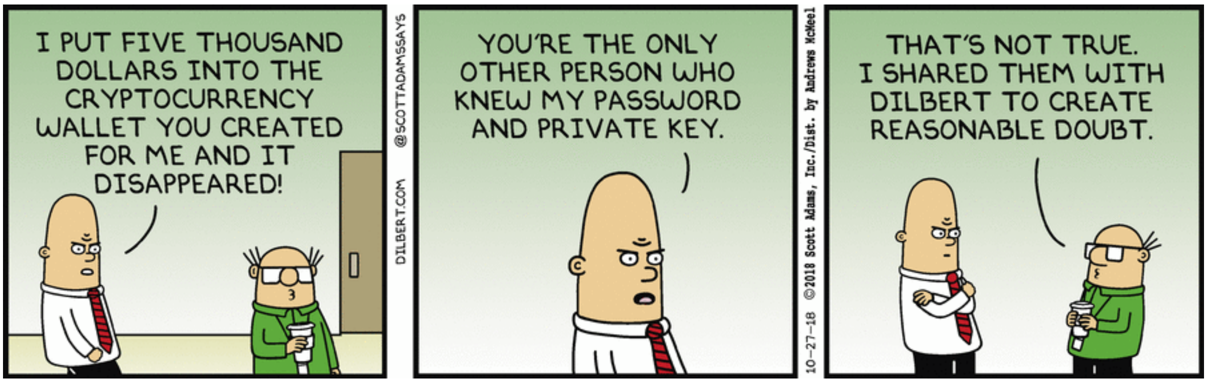

I PUT FIVE THOUSAND DOLLARS INTO THE CRYPTOCURRENCY WALLET YOU CREATED FOR ME AND IT DISAPPEARED!
@SCOTTADAMSSAYS
DILBERT.COM
YOU'RE THE ONLY OTHER PERSON WHO KNEW MY PASSWORD AND PRIVATE KEY.
10-27-18 ©2018 Scott Adams, Inc./Dist. by Andrews McMeel
THAT'S NOT TRUE. I SHARED THEM WITH DILBERT TO CREATE REASONABLE DOUBT.

FIGURE 6 – private key2

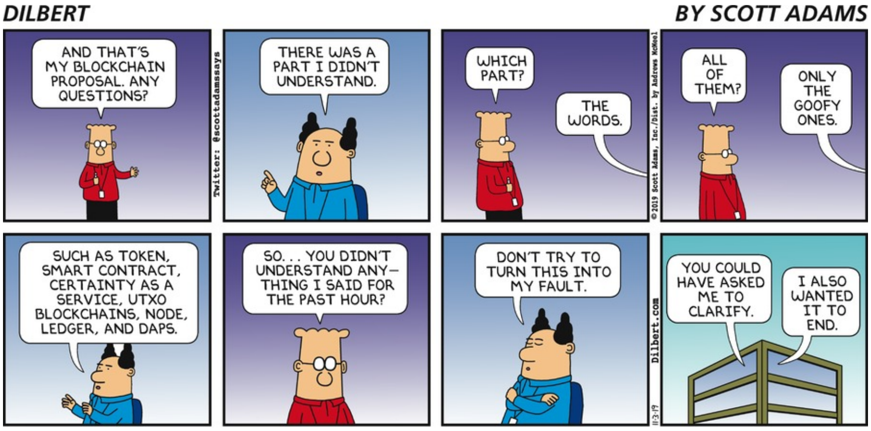

DILBERT
BY SCOTT ADAMS
AND THAT'S MY BLOCKCHAIN PROPOSAL. ANY QUESTIONS?
Twitter: @scottadamssays
THERE WAS A PART I DIDN'T UNDERSTAND.
WHICH PART?
THE WORDS.
©2019 Scott Adams, Inc./Dist. by Andrews McMeel
ALL OF THEM?
ONLY THE GOOFY ONES.
SUCH AS TOKEN, SMART CONTRACT, CERTAINTY AS A SERVICE, UTXO BLOCKCHAINS, NODE, LEDGER, AND DAPS.
SO... YOU DIDN'T UNDERSTAND ANY-THING I SAID FOR THE PAST HOUR?
DON'T TRY TO TURN THIS INTO MY FAULT.
Dilbert.com
YOU COULD HAVE ASKED ME TO CLARIFY.
I ALSO WANTED IT TO END.

FIGURE 7 – goofy words