16

The Blockchain

THE WORD PUZZLE PUBLISHING ANALOGY

Jess opens the door to the familiar garden shed.

"Busy?" she asks.

The fastidious book-keeper gnome just shakes his head in contempt as he continues his work. He is at his desk, hunched over a sheet of paper, a pile of which lies close by, ready to be checked just like a teacher marking a test. One of the fax machines purrs as usual with incoming sheets of paper.

"Here," says Jess as she hands him her latest payment.

He grabs his thick ring-binder, flicks through it, checks a few pages, and nods.

As he gets up to feed Jess's latest transaction into the second fax machine, Jess looks at the open page in the ring binder. It reads:

Official Update: 2,499.
Difficulty Adjustment = Medium [2x2, 2x3]
Solved by: Miner49er :
Last update: cdfaawvlmto.
This update: phmdmclayb.

1. **3162-5474-0260-5030 sends 1617-5301-8276-4920**
$11.34

31	62	54	74	02	60	50	30
h	p	n	t	(vowel)	o	m	h

16	17	53	01	82	76	49	20
d	e	n	(vowel)	u	t	m	e

"Phantom haunted me." [3 words]

2. **0199-1462-7374-5260 sends 4732-182350395471**
$109.50

01	99	14	62	73	74	52	60
a	(vowel)	d	p	s	t	n	o

47	32	18	23	50	39	54	71
l	h	e	e	m	i	n	s

"Dolphins, manatees." [2 words]

3. **4632-0727-5011-2839 sends 4847-0110-6868-5333**
$2.00

46	32	07	27	50	11	28	39
l	h	(vowel)	g	m	c	g	i

48	47	01	10	68	68	53	33
l	l	(vowel)	b	r	r	n	i

"Chargrilling lamb." [2 words]

4. 0971-2493-5602-7333 sends 6916-7779-4017-7670 $3,844.00

09	71	24	93	56	02	73	33
b	s	f	y	o	(vowel)	s	i

69	16	77	79	40	17	76	70
r	d	u	u	j	e	t	r

"Adjust your briefs" [3 words]

Reward for creating official update = $288,967.
End of Official Update.

Jess is curious. She has heard that certain fastidious book-keepers compete to solve puzzles. This looks like some kind of puzzle.

"How does it work? The puzzles... for the official updates?" asks Jess, as the fastidious book-keeper gets back to his seat.

The fastidious book-keeper seems surprised for an instant. "Oh, you'll need this," he says, recovering his blank expression.

The fastidious book-keeper gets up and looks on his shelves. He fetches a piece of cardboard but as he hands it to her, he says:

"Of course, don't bother trying. The official publishers are so good at it that you won't have a chance."

"Won't have a chance at what?"

"Solving the puzzle ahead of anyone else. Quickest wins everything. Look at the reward..."

Jess reads the last line of the official update again: Reward for creating official update... almost $300 grand!

Jess thinks of what she could do with all that money. "Is that for every puzzle solved?"

“More or less.”

‘Maybe if I could solve just one puzzle,’ Jess fantasizes. She looks at the piece of cardboard.

(A,E,I,O,U)	B	C	D	E	F
01,02,03,04, 05,06,07	08,09,10	11,12,13	14,15,16	17,18,19,20, 21,22,23	24,25,26
G	**H**	**I**	**J**	**K**	**L**
27,28,29	30,31,32	33,34,35,36,37, 38,39	40,41,42	43,44,45	46,47,48
M	**N**	**O**	**P**	**Q**	**R**
49,50,51	52,53,54	55,56,57,58, 59,60,61	62,63,64	65,66	67,68,69,70
S	**T**	**U**	**V**	**W**	**X**
71,72,73	74,75,76	77,78,79,80, 81,82,83	84,85,86	87,88,89	90,91
Y	**Z**	**(A,E,I, O,U)**			
92,93,94,95	96,97,98	99			

“I don’t get it.”

The fastidious book-keeper has resumed his ‘teacher marking tests’ activity and says coldly:

“If you don’t get it, I don’t have time to explain it to you, sorry.”

Jess takes the hint and leaves.

(Later that night…)

It’s been two hours worth of research but Jess finally understands how the puzzle works.

Basically, one derives letters from debit card numbers and needs to make words from them. One must use every letter one gets, no more, no less. The words must be connected in topic. That’s why ‘dolphins, manatees’ works but ‘dolphins, emanates’ does not.

Here are the rules in more detail:

1. Gather four recent transactions. They must NOT already be in the official transaction log.
2. Take ONE of the transactions and set out all the numbers of the two debit cards in a row. There will be 32 numbers.
3. Divide the row every two digits along. So, e.g. 4545-3322 becomes 45|45|33|22.
4. For each of the new 2-digit numbers, get the letter code, e.g. 45 = K, 66=Q (see previous page)
5. Now you have 16 random letters.
6. You must use every letter to make some words.
7. You are free to make two words or three words; sometimes you are allowed to make four words– see step 9.
8. The words must be connected by topic, but it can be any topic.
9. Consult the *Difficulty Adjustment.* This tells you how many two word and three word answers you are allowed in total, and whether a four word answer is allowed.
10. Repeat the steps for the remaining three transactions, i.e. go back to step 2.
11. Double check that you have not used too many two or three word answers– see step 9.
12. When you have a correct set of four answers, send it off by fax to everyone.
13. However, if someone else's correct puzzle comes in by fax before you have finished, tough luck, all your effort was in vain.

Jess practices the puzzle but with a simpler set of numbers: **3162-5474-0260.**

First, she separates the numbers into 2-digit pairs: **31|62|54|74|02|60**

Now she finds the letter codes for each of these with the cardboard 'code sheet' which the fastidious book-keeper

gave her.

31	62	54	74	02	60
h	p	n	t	(vowel)	o

Jess then makes a smart decision. Because she is practicing with fewer numbers, and so has fewer letters to work with, she will try to find just one word. It would be extremely difficult, perhaps even impossible, to get more words out of that list.

She notices that she has a 'P' and an 'H'.

"Hmm," she thinks, "lots of words start or end with a 'PH'. I'll try starting a word with 'PH'."

Ph...

"Should be a vowel next. I'll use the **o**, just because it's the one I definitely have to include. May as well try it."

Pho...

The number **02** allows any vowel. That's a big help.

After a few minutes Jess has an answer. Maybe it's just one correct answer of several. That doesn't matter. So long as you get a word which uses the *exact* amount of letters, it's fine.

Did you get an answer too?

Jess's answer is: photon.

SCRABBLE, NOT JIGSAW PUZZLE

For this example, I don't think you would have found any other answer but the one above. But with 16 letters, there are often several correct possibilities. So you need to realize something very important about this whole process:

> **There is no single correct answer. You make whatever words you can.**

Not a lot of people understand this. You might have heard that, in crypto, computers compete to 'solve a puzzle'. You now know that it's not like a jigsaw puzzle. It's like Scrabble or Balderdash. It doesn't have only *one* correct solution. You

have to follow the rules. There is a correct way to proceed. Nevertheless, your answer is not necessarily the same as another person's. At any rate, the whole business starts with choosing four recent transactions. Different people choose different transactions. That will generate different letters. Answers can't help be different with different inputs.

There is a *difficulty adjustment.* Finding two words out of the letters is usually just as hard as finding three words. The key is to have options. If you have two chances of finding two words and two chances of finding three words, then you have flexibility. One set of letters might yield three words easily. Remember that they have to make sense. They have to be of the same topic. The best thing is when there is a four word option. If you're really struggling to find two or three, then four might work.

The difficulty adjustment changes every two weeks. That happens when the puzzle-solvers complain that things are too hard. There's an inbuilt mechanism. Complaints are not enough. The average time taken to solve a puzzle is calculated. Longer than a certain time, and the difficulty is reduced.

This has a nice side effect too. Imagine there's just three people competing. Now, one hundred people suddenly join the game. What would happen to the average time? It would almost certainly go down. More people, more brains, more answers. The difficulty adjustment would then go up. The puzzles must be hard to solve in an absolute sense. Remember that the aim of the game is not to solve puzzles. The aim of the game is to verify transactions in a democratic way. The puzzle-game is a means to an end. Puzzle-solvers can band together to try to win money easier, but they soon realize that the game is not about them.

The puzzles are hard to solve. But once that fax machine purrs and an answer comes in, you can check very quickly whether it's right.

If it's right, then it goes in the ring binder. That makes it *official.*

THE CHAIN

One more thing to note:

Last update: cdfaawvlmto

This update: phmdmclayb

This serves as a synchronizing mechanism. 'Phmdmclayb' is not the latest drug from Pfizer. It's all the first letters of the words in correct order. P for 'phantom', 'H' for 'haunted', M for 'me', D for 'dolphins', M is for 'manatees', etc. When the next update comes in, it *must* have:

Last update: phmdmclayb

If it doesn't have this, then something has gone wrong. This string of letters proves that everyone is 'singing from the same hymn book' so to speak.

It's statistically impossible that any other set of words could have made that sequence of letters, given the available recent transactions. Remember that you must only use transactions checked but not yet included in the official update. That reduces the options enough for it to be statistically impossible for a coincidence.

THE REALITY: HASHING ALGORITHMS

Now to the real world. No cryptocurrency uses my '16 letter method'. Computers use pure mathematical puzzles called *hashing algorithms.* The math is way beyond me and I risked the assumption that it's beyond you too.

Rest assured, the puzzle that I explained above is logically very similar to an actual hashing algorithm. All the basic elements are the same. For example, the first step is always to gather together some of the most recent transactions. These are transactions not entered into the official log yet. In my example I used four. Bitcoin uses about 2,000. Most importantly, the real puzzle is made up of the transaction numbers, just like in the analogy.

You're probably curious what 'hashing' is; as in 'hashing algorithm'. 'Hashing' is making a 'hash'. This is a piece of jargon in computer science. The notion is actually quite simple. A hash is a lot like running forwards between two

white lines, a hundred meters apart, and counting your steps. That's very easy. Now run backwards and land exactly on the first white line. That's almost impossible. If you don't trip over, then, even if you count your steps again, you will be extremely lucky to land on the white line without seeing it. That's analogous to how the math works for a hash. When you input something, you get an output very easily. But if you start with the output, it's very, very difficult to get the input.

You might like to imagine the puzzle-game using this analogy. Imagine the official publishers all running backwards and trying to land on a circle the size of a golf ball. Imagine too that they're not even given an exact amount of steps. "Between 2,000 and 3,000." This would be so hard that they'd just have to try and try, over and over. That's what happens with bitcoin. The amount of attempts to find a correct answer ends up in the quintillions. That's a number with 18 zeroes.

We will stick to my 16 letter algorithm. Unless you plan on being a computer programmer, it's sufficient.

THE MERITOCRATIC WAY FOR WHO GETS THE SAY

Augustus, the first Roman emperor, said that he was 'first amongst equals'. *Primus inter pares.* Translation: "We're all equal here, but what I say goes."

When you give one member of a team special privileges, that member tends to take over. Satoshi Nakamoto designed a system of money with equal-powered participants. He knew that he couldn't give any member special powers. No fastidious book-keeper can pull rank. There are no ranks! That would be a recipe for turmoil. Even rotating the honor amongst a few book-keepers would be dangerous. It could lead to corruption. Even a single dispute can cause a wound that festers.

Satoshi wanted to avoid 'office politics' at all cost. The only way to sort out office disputes is for the boss to step in. But with a decentralized, voluntary system, there is no boss. Satoshi wasn't a Pollyanna however. He knew that disputes

occur, and often. He realized that the only fair way was to make it a *meritocracy.* Every official update to the transaction log was to be a competition. Any fastidious book-keeper could compete. The rules were the same for all. One gathered up a bunch of transactions, and then raced to complete a puzzle. When one got his or her answer and it made sense according to the rules (analogous to my 16-letter puzzle stated above), one sent it out to all the other fastidious book-keepers. First valid answer wins the round.

This is a lot to take in, so let me summarize the process again, within the analogy used in this book.

1. New transactions since the last official update come in on the fax machine.
2. Fastidious book-keepers double-check them.
3. A subset of fastidious book-keepers compete to solve a puzzle with some of the new transactions. They are called the *official publishers.*
4. The official publishers each gather up (any) four of the new transactions (in reality about 2,000) and derive a fixed amount of 2-digit numbers from them.
5. They follow very specific rules of the game which make it quite easy to check whether one has answered correctly or not.
6. They have to consult the difficulty adjustment.
7. Either an official publisher completes the puzzle before anyone else and sends it out, or sees a correct page of answers from another official publisher arrive by fax, and then– so long as it really is correct– has to give up on that round.
8. The winning official publisher gets a reward.
9. The correct page is put in the ring binder and

becomes the *official update*. It has the first letter of all the words of the previous update to make sure things are in order.

10. If the sequence of letters from the words of the previous update do not match, something has gone wrong, and the page is put in a pile labelled 'orphans'.
11. Repeat from step 4 until a synchronization occurs.
12. Transactions from the orphan pile are used again in new rounds. Sooner or later they all make it in the official transaction log.

I hope it makes sense, but you might have to read this chapter a couple of times. Take heart in the fact that, if the system wasn't so difficult to grasp at first, someone would have thought of it before.

It's a brutal system in a way because there is no compensation for second place. There is no reward for working ten years as an official publisher. There is just the next round of 'winner take all'.

GUESSWORK IS NOT EXACTLY MERITOCRATIC

Some may object to my calling of the system 'meritocratic'. That implies skill. The word 'merit' comes from the Latin word for 'deserving'. There is some skill in finding meaningful words from 16 letters, but a lot of guesswork too. In the actual hashing algorithms which computers use, it's almost all guesswork.

I still think that it's a meritocratic system, broadly speaking, because, for example, faster CPUs in the computers mean more chance of winning. They can make more guesses per second. It's like a stronger person winning the sprinting race.

Perhaps *victorocratic*, from the Latin for 'winner' is more accurate.

There was another reason why Satoshi chose such a system.

It goes beyond the reason of office politics, corruption, and so forth. That's a big concern, but it's not like all centralized organizations become as decadent as Nero's Rome. Visa and Mastercard might not be perfect, but they work pretty well. Satoshi even admitted as much in the introduction to the whitepaper.

I think the fate of **e-gold** had an influence on Satoshi.

Of all the online monetary systems before bitcoin, e-gold was probably the most successful. The idea was simple. The e-gold company had a lot of gold in vaults. They made units in a database; these corresponded to 1 gram of gold each. People logged in to the e-gold website and bought these units of gold. They could trade with other users. The fact that they were trading numbers in a database made it instantaneous over the Internet. At its peak in the mid noughties e-gold was doing 2 billion dollars worth of business per year.

C.E.O. Dr. Douglas Jackson bent over backwards to act within the U.S. laws. Alas to no avail. The F.B.I. raided his vaults in 2007 and seized a ton of gold. They charged Jackson with being an illegal money transmitter. There was a bank-run on e-gold and it never recovered.

2007 was the year when Satoshi was working on the idea of bitcoin. He must have realized that to centralize an online form of money was to make it a sitting duck. The story of e-gold was chilling because the F.B.I. seized the gold *before* the company was found guilty of any crime.

Even if there was no gold behind bitcoin, it was still too much to make it all hinge on a few really powerful computers. That might mean that sooner or later... *plunk!* That's the sound of a power cable being unplugged.

THE REAL BLOCKCHAIN TERMINOLOGY

You already understand the blockchain better than most people who own crypto.

You just have to understand how to translate my analogy...

MOLINO'S ANALOGY	*CRYPTO REALITY*
Jess's transaction messages	*'tx' message on a TCP port*
page of official update	*block*
sequence of all the first letters of the words used to solve the puzzle	*'Merkle Tree' hash of all the transactions in the block*
last update's sequence of first letters and this update's sequence of first letters	*chain of 'Merkle Tree' hashes*
word puzzle	*hashing algorithm (bitcoin uses one called 'SHA-256')*
fastidious book-keeper	*node (computer program)*
official publisher	*miner/validator*
the ring binder of the official updates in order	*full blockchain*
difficulty adjustment	*difficulty adjustment*
2x2, 2x3 words	*range of possible valid numbers as result of hashing*
fax machine	*Internet, delayed by the computer program to prevent advantages of faster connections.*

Computers don't use sheets of paper for information– obviously– and documents like you use in word-processing software would be overkill for basic Internet traffic.

Instead, cryptocurrencies use *blocks*.

WHAT ARE BLOCKS?

Blocks are just a big bundle of financial transactions, the kind you are already well-familiar with:

0971-2493-5602-7333 sends 6916-77794017-7670
$3,844.00

Actually, it's more than just the bundle of financial transactions. A bundle could, in theory, have fake transactions in it. What if one of the transactions was like this?

dumb-arse-5602-7333 sends rich-prat-4017-7670
$3,844.00

Can't be. The fastidious book-keepers have all checked it first. This one wouldn't get though the front gate. The official publishers are book-keepers too. They check again. Plus, those letters wouldn't work in the puzzle-game.

So it's better to say that a 'block' in terms of the 'blockchain' is a bundle of valid transactions.

It's even more than that.

Remember the 'chain' part? [→**THE CHAIN**] Those letters 'Phmdmclayb' acted as a serial number. They sync up with the last block and the next block. That makes the chain. That's so important, because it prevents fraudulent transactions. I mean, it prevents people claiming that they have money when they don't.

Valid transactions make up a block.

Valid blocks make up a transaction history.

A valid transaction history makes up a trustworthy system.

You can be sure that a person sending you crypto money has that money. Why? Because there's a record of all transactions going back to the moment the cryptocurrency came into being.

It's like a certificate of authenticity for silver. Imagine Jane just sent you a 1oz silver coin. Jane got it from Pete who got it from Amanda who got it from Xavier. Xavier mined the silver in 2009. There is a 'chain' going back to the coin's

origin. You can easily check it, before you accept Jane's coin.

It's just that cryptocurrency does it better.

In the above example, the silver coin has an official record. It's a chain of custody. That's good, but far from perfect. What if one of the records was forged? What if someone could bribe an official to change a name? The silver mine → Xavier → Amanda → Pete → Jane → you, allegedly. What if *Jake* got it from Pete, but the official who does the documentation changed one letter to make 'Jake' = 'Jane'?

With a blockchain, that can't happen.

In a blockchain, each record earns its keep. I mean: Every transaction on every page contributes to the proof that the page is valid. As amazing as it sounds, for the 1.1 billion transactions of bitcoin ever, if a *single* transaction was wrong, it would invalidate *all* of them!

In the above example, the corrupt official changed 'Jake' to 'Jane'. That single letter change would ruin that block which would ruin the previous block which would ruin the previous block, and so on back to the beginning.

How does that work? Good news: You already know.

Let's stick with my analogy. You can see that...

0971-2493-5602-7333 sends **6916-7779-4017-7670**
$3,844.00

... can be trusted. How exactly? You work backwards:

"Adjust your briefs"

... can be checked for each letter's code. Consult the letter-code chart on page 155. You need to break the debit card numbers down into pairs first...

09|71|24|93|56|02|73|33|69|16|77|79|40|17|76|70.

Now check the code.

Those numbers equal the following letters:

b, s, f, y, o, [a/e/i/o/u], s, i, r, d, u, u, j, e, t, r.

All of those 16 letters are used in 'adjust your briefs'. If even one number of those debit cards was different, it wouldn't work; you couldn't get 'adjust your briefs'. A miss is

as good as a mile.

If you imagine that the name 'Jake' was used in the phrase which won the puzzle game, you can understand why changing it to 'Jane' would invalidate the block.

Let's call those groups of first letters that link the blocks together *letter-hashes.* One letter-hash is 'Phmdmclayb'. The letter-hashes come in with the updates. For example...

TIME	BLOCKCHAIN LINK
10.52	cdfaawvlmco → phmdmclayb
11.02	phmdmclayb → trfdyaulvl
11.11	trfdyaulvlf → rgthajbil
(etc.)	(etc.)

This is the actual chaining-together of blocks, or the 'blockchain'. To change one number in a transaction is to change the letter-hash. Then the letter-hashes don't sync up. The chain is broken. You can see now why destroying just one transaction in bitcoin would destroy the whole system, right back to bitcoin's moment of creation!

It's the most demanding system of verification in the history of mankind.

SIMULTANEOUS PUZZLE SOLVING

Can two official publishers solve a puzzle at the same time? Yes, this can happen for sure. A fastidious book-keeper can receive two correct solutions almost simultaneously. In our analogy, the fax machine would start on the second page as soon as it spat out the first page. In the real world, the *nodes* would receive two correct solutions within a few milliseconds.

Remember that the blockchain puzzle-game is not like a jigsaw puzzle. There's not just one possible answer. So, when two different solutions come in at the same time, there are now two equally valid updates, but they have different

letter-hashes.

There's a clever procedure to solve this. First one wins. But that's not the clever part. The second one, the almost-winner, is kept in a pile, called 'orphans'. It may still make a comeback.

Let's call the two correct solutions 1-A and 1-B. 1-B is in the orphan pile because it came in a fraction too late. When the next answer comes in, answer 2, it will *either* sync up with 1-A or 1-B. It can't sync up with both. The transactions and letter-hashes will be different. Whichever one it syncs up with wins. It does not matter if you have to pull out the top page from the ringbinder.

> **The chain must sync up. If not, you must pull out the updates and replace them with the newest updates which *do* sync up.**

There is a very good reason why it's done this way.

Fastidious book-keepers are distributed all over the world. If there are two simultaneous correct solutions then some will get answer 1-A first and some with get answer 1-B first. The fastidious book-keepers will temporarily split into two teams: Team A, Team B.

This is potentially a disaster. Team A has the official transaction log with the 1-A page, and Team B has the official transaction log with the 1-B page. When you have a database and people are supposed to be using the same database, but they aren't, it's chaos.

It's not a Roman-Emperoresque, *primus inter pares* system. No one can pull rank. Both teams must just wait for the next update. It will either match 1-A, so Team A has the right chain, or 1-B, so Team B has the right chain. The team with the wrong chain will have to pull out the wrong update and put in the correct one. Good thing they kept an orphan pile! It's a simple system but one that prevents arguments and ambiguity.

Realistically, at very most, two blocks will have to be replaced. Simultaneous puzzle solutions are rare. One

occurs, sure, but then a second? Maybe. Three? No chance.

In my analogy, the fastidious book-keepers would never have to replace more than the top two pages.

THE BLOCKCHAIN IS NOT THE ANSWER TO EVERY PROBLEM

'Blockchain' has become a buzzword.

Many times, people in the business community use the term without a true understanding. They use it to mean something like 'trendy new database technology which might have a Midas touch.'

Blockchains are not the answer to everything.

For one thing, they are slow compared to centralized databases. Just think of all those fastidious book-keepers competing to solve problems and then possibly reversing a correct solution or two. One big mainframe fridge of a server doesn't have this malarky. Democracy is messy.

Also slow is their time to maturity. To grow, people all over the world have to commit their computers and electricity costs. They have to realize the advantages. They have to see that disagreements and external attacks do not stop the blockchain.

These days Venture Capital firms often throw a ton of money at new blockchains to speed things up. This 'astroturfing' has not worked so far. There's too much competition and too little loyalty. The V.C. money buys a few months of fame, but that's not nearly enough. It takes at least ten years for a true blockchain to mature.

This fact is in stark contrast to the popular perception of crypto as a 'get rich scheme'.