The Blockchain Game - Simplified Version

J Scott Christianson
Byron Rich and Janyl Jumadinova

Miner Instructions

Hash = Nonce + a + b + c - Value of Last 2 digits of prev Hash

a = Value of the first letter of the course
b = Value of the first letter of the student Public Key
c = Value of the Grade

Nonce = value between 1 and 3 that you will adjust to calculate a hash that can be equally divisible by 3

Lookup Table

A	65	N	78
B	66	O	79
C	67	P	80
D	68	Q	81
E	69	R	82
F	70	S	83
G	71	T	84
H	72	U	85
I	73	V	86
J	74	W	87
K	75	X	88
L	76	Y	89
M	77	Z	90

Our First Block - This is enough info to start. Use the formula from the previous sl

Block	Course	Student	Grade	Nonce (1-3)	Prev Hash	a	b	c	Hash
									212
1	Parks 320	ad59da	F		12	80	65	70	

Subsequent Blocks - Fill in the table

Block	Course	Student	Grade	Nonce (1-3)	Prev Hash	a	b	c	Hash
									212
1	Parks 320	ad59da	F						
2	Engineering 300	bd9ebc	B						
3	Business 200	c67445	C						
4	Parks 320	e2dd8a	B						
5	Engineering 300	e2dd8a	D						
6	Engineering 300	bde7af	B						

Subsequent Blocks - Fill in the table

Block	Course	Student	Grade	Nonce (1-3)	Prev Hash	a	b	c	Hash
									212
1	Parks 320	ad59da	F	1	12	80	65	70	204
2	Engineering 300	bd9ebc	B	1	4	69	66	66	198
3	Business 200	c67445	C	3	98	66	67	67	105
4	Parks 320	e2dd8a	B	3	5	80	69	66	213
5	Engineering 300	e2dd8a	D	2	13	69	69	68	195
6	Engineering 300	bde7af	B	2	95	69	66	66	108

Questions?

- Anyone, what courses did `c67445` take and what grade did they earn?

What if….

- We change block 1 as follows….

Block 1

Course: Parks 320

Student: ad59da

Grade: F -> A

What if….

- A grade is announced by someone other than a faculty member?
- Student pays off a node (any node) to record an A in for their grade?
- A student’s private key is lost?

What if….

- A miner changes a transaction and announces the hash to the network before anyone else calculates it?
- The difficulty of calculating a hash increases as the blockchain grows?

Try this table in groups.

Block	Course	Student	Grade	Nonce (1-3)	Prev Hash	a	b	c	Hash
									461
1	Art 181	ad3614	A						
2	Bio300	cm2197	B						
3	Chem200	mf3996	C						
4	WGSS320	rd4201	D						
5	CMPSC 300	qs6009	A						
6	Psych300	zz3001	F						

Results?

Block	Course	Student	Grade	Nonce (1-3)	Prev Hash	a	b	c	Hash
									461
1	Art 181	ad3614	A	1	61	65	65	65	135
2	Bio300	cm2197	B	1	35	66	67	66	165
3	Chem200	mf3996	C	1	65	67	77	67	147
4	WGSS320	rd4201	D	2	47	87	82	68	192
5	CMPSC 300	qs6009	A	2	92	67	81	65	123
6	Psych300	zz3001	F	2	23	80	90	70	**219**

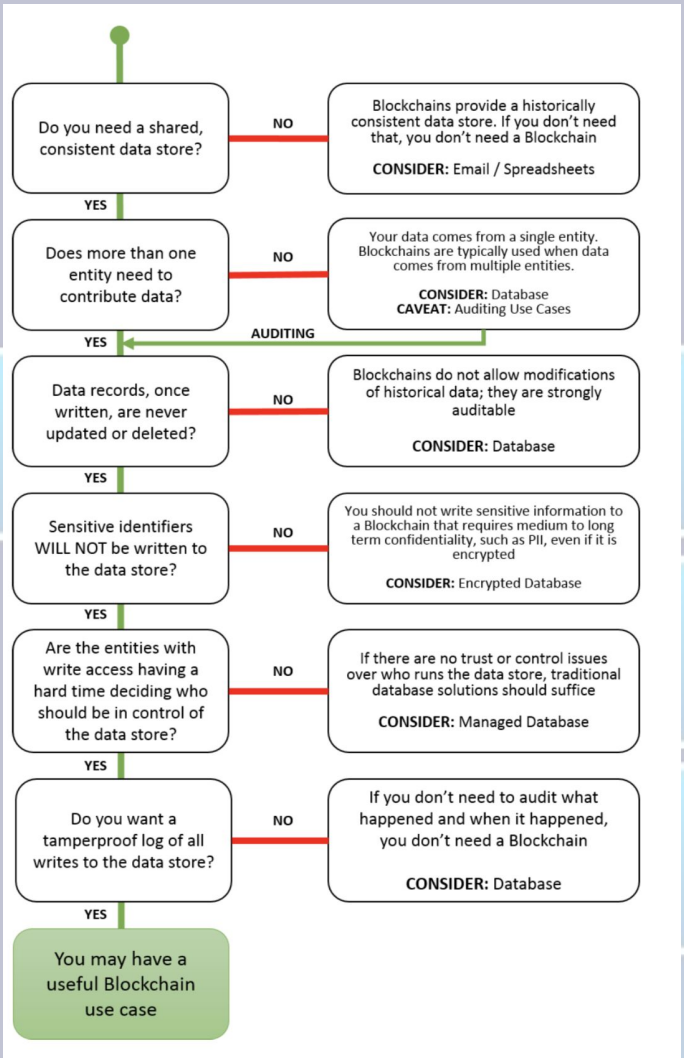
What did we observe in this “Game”

- Distributed Ledger
  - No central authority to hold ledger or be attacked.
  - All people (aka nodes) have complete ledger.
- Transparent but anonymous Ledger
  - Ledger can be public while concealing identity.
- Append only Ledger
  - Each entry (aka block) is linked to the previous entry via some math (aka hash).
  - Some nodes (aka miners) are paid for performing calculations (aka proof of work).
- Immutable Ledger
  - Attacks to ledger are impractical due to need for majority of nodes (aka 51% attack) to agree to a change and the computational power required.

Grade Blockchain

- While a grade blockchain provides a good exercise to explain blockchain in a class, storing grades is probably not a great application for blockchain.
- What are good applications for blockchain? I recommend the DHS flowchart to get you started.

The Blockchain Game



Review

- Distributed Ledger
  - No central authority to hold ledger or be attacked.
  - All people (aka nodes) have complete ledger.
- Transparent but anonymous Ledger
  - Ledger can be public while concealing identity.
- Append only Ledger
  - Each entry (aka block) is linked to the previous entry via some math (aka hash)
  - Some node (aka miners) are paid for performing calculations (aka proof of work)
- Immutable Ledger
  - Attacks to ledger are impractical due to need for majority of nodes to agree to a change and the computational power required.