The Blockchain Game

J Scott Christianson

Blockchain Basics

- A Distributed Ledger
  - No central server or authority.
  - Everyone (aka node) on the network has a copy of the ledger.
  - A huge variety of information can be stored on a blockchain ledger.

Blockchain Basics

- A Distributed Ledger Can Store:
  - Financial Transactions
  - Property Records
  - Shipments and Inventory
  - Grades????

Blockchain Basics

- A Distributed Ledger For Grades
    - All teachers calculate student grades and then enter the grades into a central repository (the registrar or central office).
    - Why not eliminate the registrar (save some $$) and just have the teachers maintain the ledger of grades?

The Grade Blockchain

- Let’s try it!
  - Everyone in the class will act as “special” nodes called “Miners.”
  - I will pick on seven people to be “students”

The Grade Blockchain

- Student identities are concealed.
  - Each student has a public ID that matches with a private ID that only the student knows.

Student ❶

Below is your key pair for the grade blockchain. Your teacher will assign a grade to your public key. You can then use any of the grade scanning tools to review the blockchain and retrieve your grades.

Public Key	Private Key
ad59da	c8fc47b6fe

Block 1

Course: Parks 320

Student: ad59da

Grade: F

Our First Block

Grade BlockChain

Block	Course	Student	Grade	Nonce (1-3)	a	b	c	Value of Last 2 digits of Prev Hash	Hash
									212
1	Parks 320	ad59da	F					12	
2									
3									
4									
5									
6									

Finishing the block: Hashing

- Miners will solve a puzzle to create a unique number for the block (aka a hash) using the information contained in our block and use that to make our ledger secure!
- First to generate a correct hash **wins**
- Other miners and nodes will verify if that hash is correct

Miners Mine!!

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

a = Value of the first letter of the course in the look up table (a=65, b=66, etc.)

b = Value of the first letter of the student Public Key in the look up table (a=65, b=66, etc.)

c = Value of the Grade in the look up table (a=65, b=66, etc.)

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

Look up 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

Grade BlockChain

Block	Course	Student	Grade	Nonce (1-3)	a	b	c	Value of Last 2 digits of Prev Hash	Hash
									212
1	Parks 320	ad59da	F		80	65	70	12	
2									
3									
4									
5									

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

Finishing the block: Hashing

1

Grade BlockChain

Block	Course	Student	Grade	Nonce (1-3)	a	b	c	Value of Last 2 digits of Prev Hash	Hash
									212
1	Parks 320	ad59da	F	1	80	65	70	12	204
2									
3									
4									
5									

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

The Blockchain Game

Block 2

Course: Engineering 300

Student: bd9ebc

Grade: B

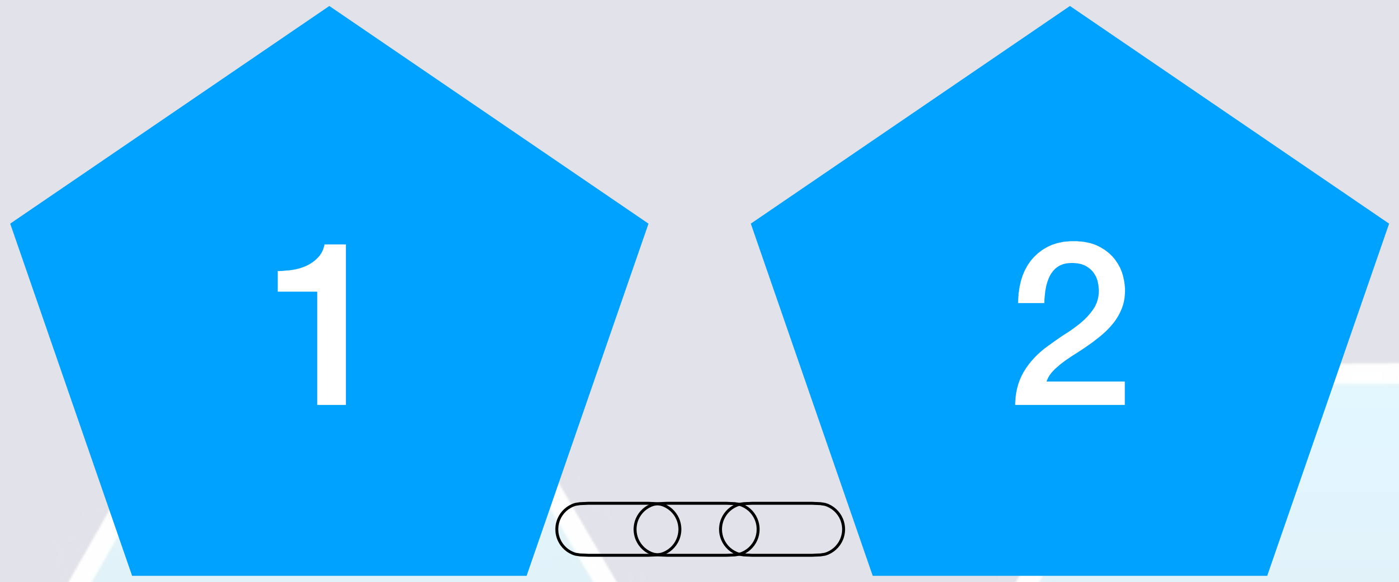
Look up Table

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

Miners Mine —> Verify and Vote —>

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

Finishing the block: Hashing



Grade BlockChain

Block	Course	Student	Grade	Nonce (1-3)	a	b	c	Value of Last 2 digits of Prev Hash	Hash
									212
1	Parks 320	ad59da	F	1	80	65	70	12	204
2	Engineering 300	bd9ebc	B	1	69	66	66	4	198
3									
4									
5									

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

The Blockchain Game

Block 3

Course: Business 200

Student: c67445

Grade: C

Miners Mine —> Verify and Vote —>

Look up 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

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

Finishing the block: Hashing

Grade BlockChain

Block	Course	Student	Grade	Nonce (1-3)	a	b	c	Value of Last 2 digits of Prev Hash	Hash
									212
1	Parks 320	ad59da	F	1	80	65	70	12	204
2	Engineering 300	bd9ebc	B	1	69	66	66	4	198
3	Business 200	c67445	C	3	66	67	67	98	105
4									
5									

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

Block 4

Course: Parks 320

Student: e2dd8a

Grade: B

Miners Mine —> Verify and Vote —>

Look up 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

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

Finishing the block: Hashing

Grade BlockChain

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

The Blockchain Game

Block 5

Course: Engineering 300

Student: e2dd8a

Grade: D

Miners Mine —> Verify and Vote —>

Look up 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

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

Finishing the block: Hashing

Grade BlockChain

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

Block 6

Course: Engineering 300

Student: bde7af

Grade: B

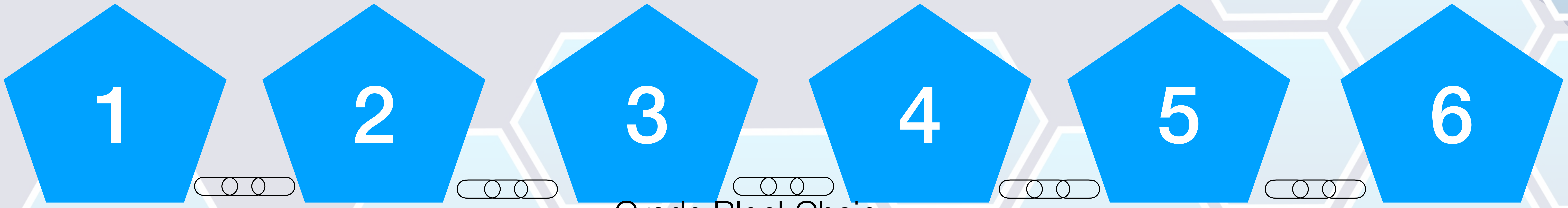
Miners Mine —> Verify and Vote —>

Look up 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

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

Finishing the block: Hashing



Grade BlockChain

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

Questions?

- Anyone, what courses did `c67445` take and what grade did they earn?
- Student 2 what grades have you received?

What if….

- We change block 1

Block 1

Course: Parks 320

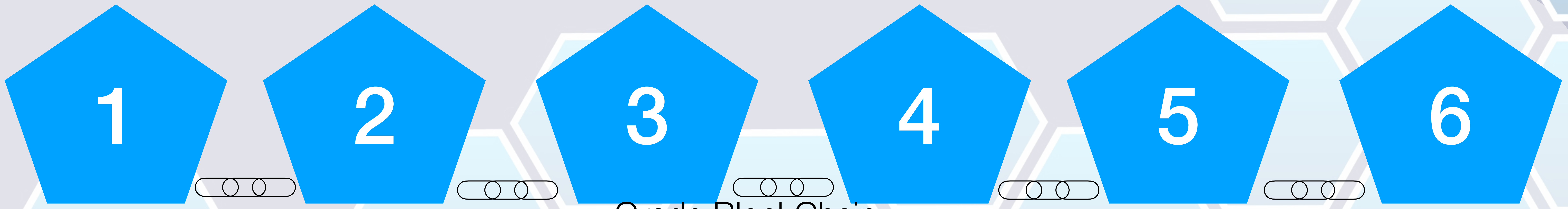
Student: ad59da

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?
- Student 5’s Private Key is lost.

Finishing the block: Hashing



Grade BlockChain

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

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?

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.

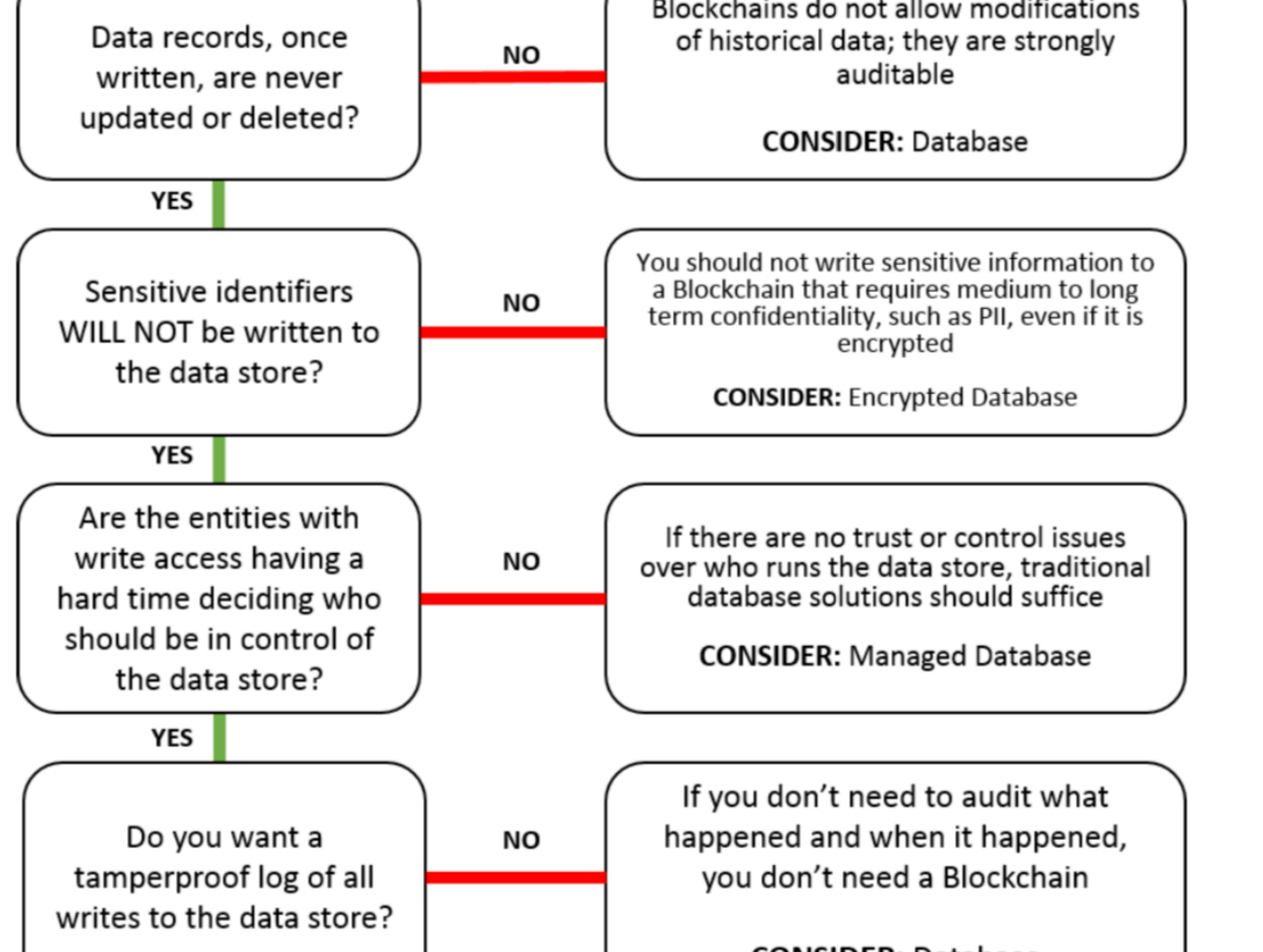
- Append only Ledger
  - Each entry (aka block) is linked to the previous entry via some math (aka hash).
  - Some nodes (aka miners) are paid for performing calculations (aka proof of work).
- Immutable Ledger
  - Attacks to ledger are impractical due to need for majority of nodes (aka 51% attack) to 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.

in Game



Data records, once written, are never updated or deleted?

NO

Blockchains do not allow modifications of historical data; they are strongly auditable

CONSIDER: Database

YES

Sensitive identifiers WILL NOT be written to the data store?

NO

You should not write sensitive information to a Blockchain that requires medium to long term confidentiality, such as PII, even if it is encrypted

CONSIDER: Encrypted Database

YES

Are the entities with write access having a hard time deciding who should be in control of the data store?

NO

If there are no trust or control issues over who runs the data store, traditional database solutions should suffice

CONSIDER: Managed Database

YES

Do you want a tamperproof log of all writes to the data store?

NO

If you don't need to audit what happened and when it happened, you don't need a Blockchain

CONSIDER: Database

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.

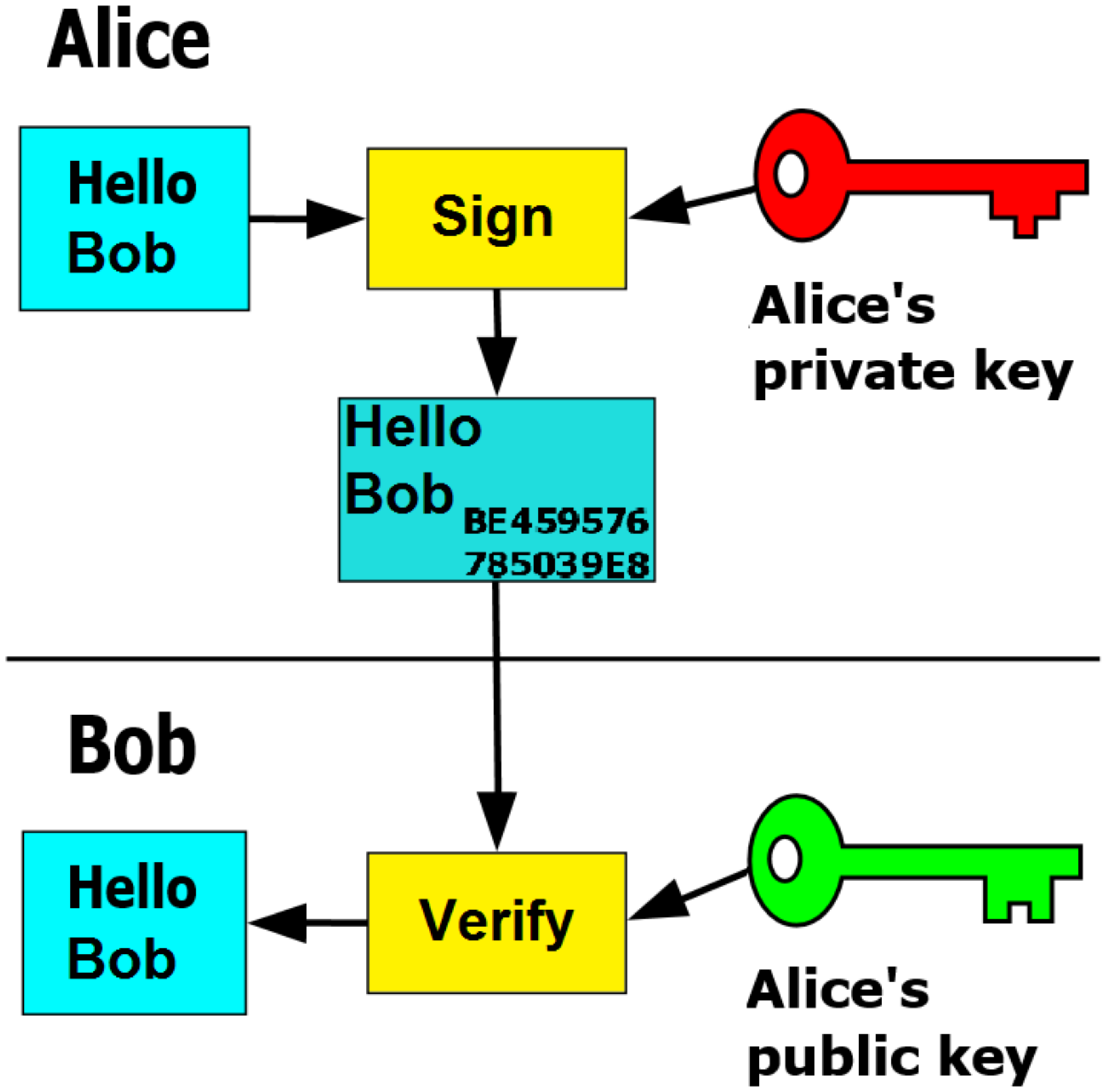
Blockchain FYI

Mid-Missouri Chapter of Internal Auditors

Public Key Encryption is an Essential Part of Blockchain

Blockchain FYI

Mid-Missouri Chapter of Internal Auditors



Public Key Encryption is also used to digitally sign transactions