Blockchain Introduction

Bryant Walker Smith

Assistant Professor
University of South Carolina School of Law
and (by courtesy) School of Engineering

Affiliate Scholar
Center for Internet and Society at Stanford Law School
cyberlaw.stanford.edu/bws

law of the newly possible
newlypossible.org

Blockchain

- A blockchain is a decentralized ledger in which each set of entries references its predecessor
- A ledger is a chronological record of transactions
- Decentralized means distributed among multiple participants rather than maintained by one

A *stylized* illustration

- Law school transcript: A *ledger* of the courses you took and the grades you earned

Course	Grade
Tort Law	A
Tort Theory	B
Advanced Torts	B
Tortes and Cakes	C
How to Commit Torts	A

Your transcript today

- *Centralized* ledger
  - Controlled by the Registrar
  - Do you trust her? (Yes: She's awesome)

Course	Grade
Tort Law	A
Tort Theory	B
Advanced Torts	B
Tortes and Cakes	C
How to Commit Torts	A

Course	Grade
Tort Law	C
Tort Theory	C
Advanced Torts	C
Tortes and Cakes	C
How to Commit Torts	C

law of the newly Possible
newlypossible.org

Your transcript today

- Your copy is just a copy
  - Controlled by you
  - Will potential employers trust you?

Course	Grade
Tort Law	A
Tort Theory	B
Advanced Torts	B
Tortes and Cakes	C
How to Commit Torts	A

Course	Grade
Tort Law	A
Tort Theory	A
Advanced Torts	A
Tortes and Cakes	A
How to Commit Torts	A

law of the newly possible
newlypossible.org

First solution

Course	Grade
Tort Law	A
Tort Theory	B
Advanced Torts	B
Tortes and Cakes	C
How to Commit Torts	A

Course	Output
Tort Law	4
Tort Theory	3
Advanced Torts	3
Tortes and Cakes	2
How to Commit Torts	4

Total: 16

Create a *function*:

- Takes your grade as an input (e.g., “A”)
- Gives a number as the output (e.g., “4”)

law of the newly possible
newlypossible.org

First solution

Course	Grade
Tort Law	A
Tort Theory	B
Advanced Torts	B
Tortes and Cakes	C
How to Commit Torts	A

Course	Output
Tort Law	4
Tort Theory	3
Advanced Torts	3
Tortes and Cakes	2
How to Commit Torts	4

Total: 16

Course	Grade
Tort Law	A
Tort Theory	A
Advanced Torts	A
Tortes and Cakes	A
How to Commit Torts	A

Course	Output
Tort Law	4
Tort Theory	4
Advanced Torts	4
Tortes and Cakes	4
How to Commit Torts	4

Total: 20

Course	Grade
Tort Law	C
Tort Theory	C
Advanced Torts	C
Tortes and Cakes	C
How to Commit Torts	C

Course	Output
Tort Law	2
Tort Theory	2
Advanced Torts	2
Tortes and Cakes	2
How to Commit Torts	2

Total: 10

But what's the problem?

- Do you want the world to know your total?
- How do we trust that your total is correct?
- How do we trust that the path to your total is correct?

Course	Grade
Tort Law	A
Tort Theory	B
Advanced Torts	B
Tortes and Cakes	B
How to Commit Torts	B

Course	Output
Tort Law	4
Tort Theory	3
Advanced Torts	3
Tortes and Cakes	3
How to Commit Torts	3

Total: 16

law of the newly Possible
newlypossible.org

Second solution

Course	Grade
Tort Law	A
Tort Theory	B
Advanced Torts	B
Tortes and Cakes	C
How to Commit Torts	A

Course	Output
Tort Law	3d873f
Tort Theory	dk3KD5
Advanced Torts	dk3KD5
Tortes and Cakes	8v298a
How to Commit Torts	3d873f

Changing the grade changes the output!

Hash

A mathematical function!

- Takes your grade as an input (e.g., “A”)
- Gives a string as the output (e.g., “3d873f”)

We’ll discuss encryption later!

law of the newly Possible
newlypossible.org

Third solution

Course	Grade
Tort Law	A
Tort Theory	B
Advanced Torts	B
Tortes and Cakes	C
How to Commit Torts	A

Course	Output
Tort Law	3d873f
Tort Theory	dk3KD5
Advanced Torts	dk3KD5
Tortes and Cakes	8v298a
How to Commit Torts	3d873f

893D90

Hash

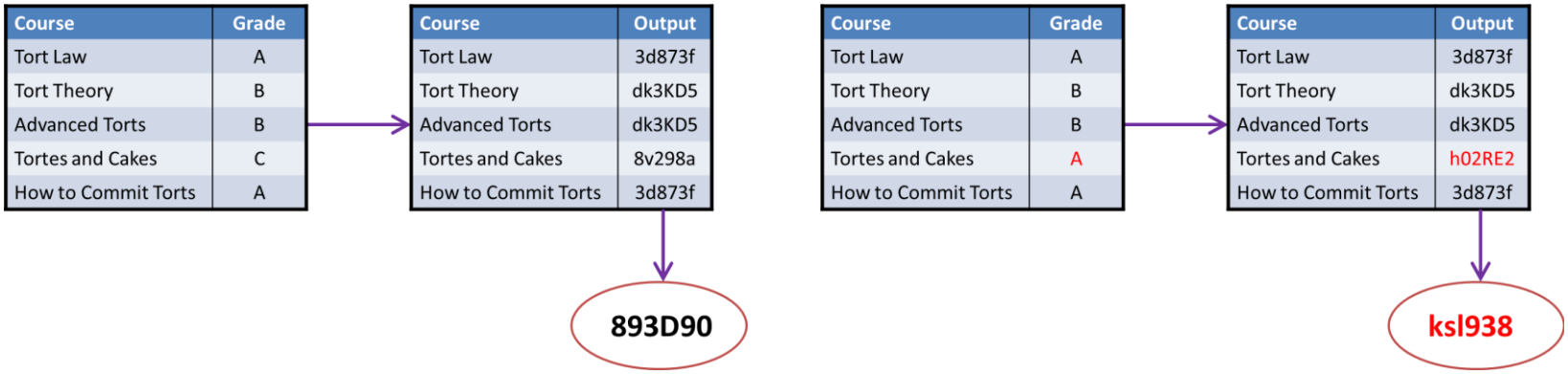
A mathematical function!

- Takes the *previous outputs* as an input
- Gives a *new* string as the output

law of the newly possible
newlypossible.org

As a result

- Changing any grade changes the corresponding output
- Changing that output in turn changes any outputs that are based on it



law of the newly possible
newlypossible.org

Third solution

- Hash *everything* (not just the grades)
  - Hash to 256 characters instead of 6 characters
  - There are **2^256** possible combinations (>100,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000)

- *Every* hashed output is now 256 characters
  - "Tort Law A" → 256 characters
  - Your entire exam answer → 256 characters
  - A file of law school blueprints → 256 characters

Refining our illustration (*still stylized!*)

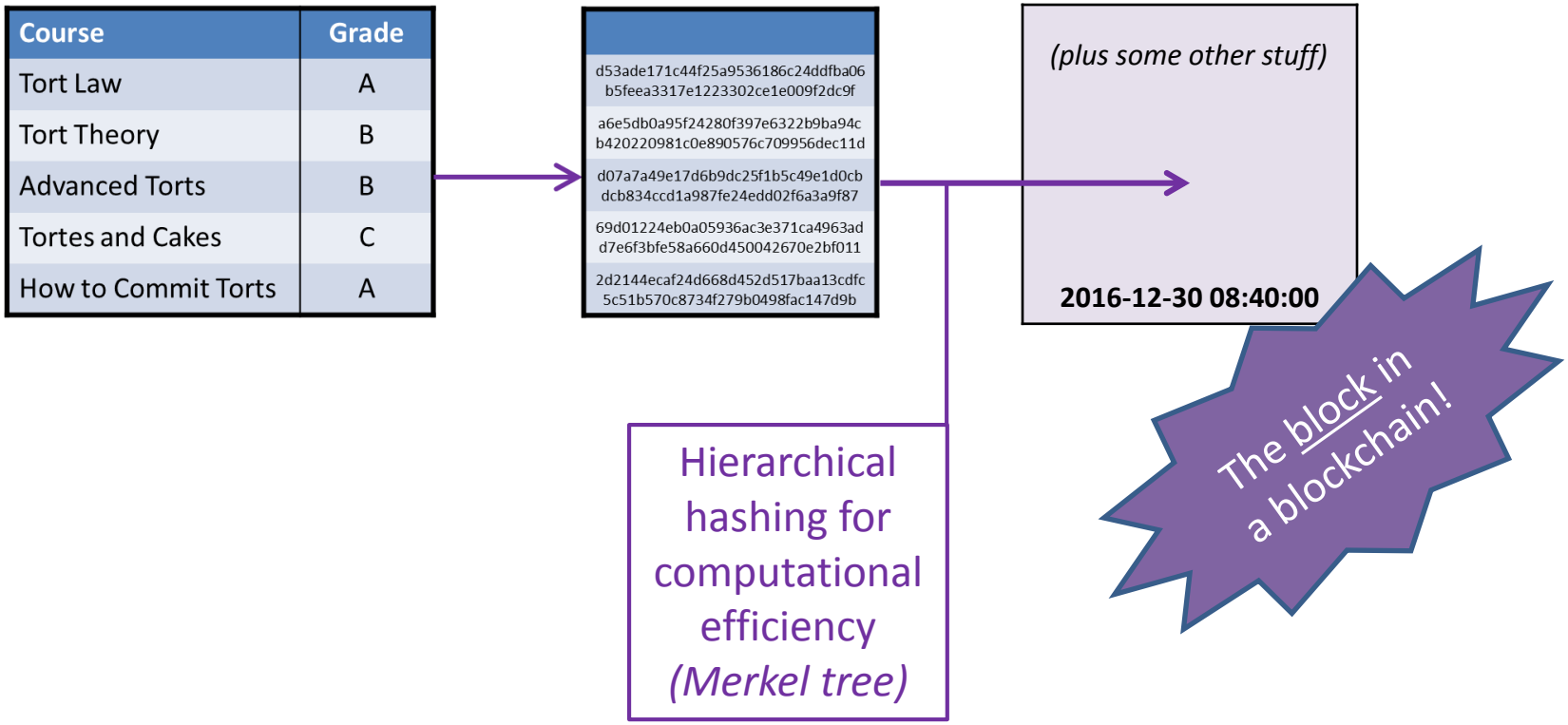
Course	Grade
Tort Law	A
Tort Theory	B
Advanced Torts	B
Tortes and Cakes	C
How to Commit Torts	A

Hash

d53ade171c44f25a9536186c24ddfba06b5feea3317e1223302ce1e009f2dc9f
a6e5db0a95f24280f397e6322b9ba94cb420220981c0e890576c709956dec11d
d07a7a49e17d6b9dc25f1b5c49e1d0cbdcb834ccd1a987fe24edd02f6a3a9f87
69d01224eb0a05936ac3e371ca4963add7e6f3bfe58a660d450042670e2bf011
2d2144ecaf24d668d452d517baa13cdfc5c51b570c8734f279b0498fac147d9b

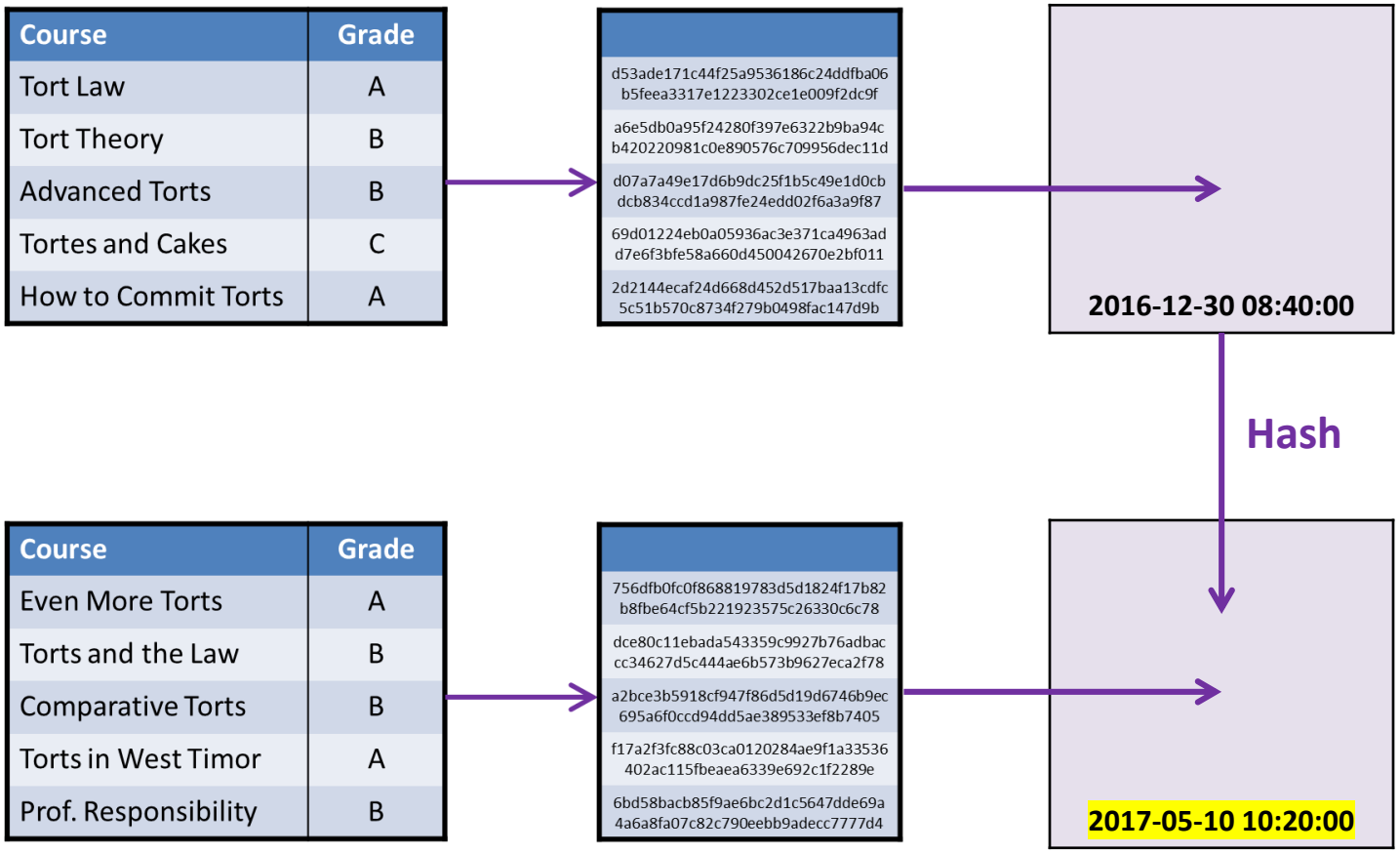
(using SHA-256)

Refining our illustration



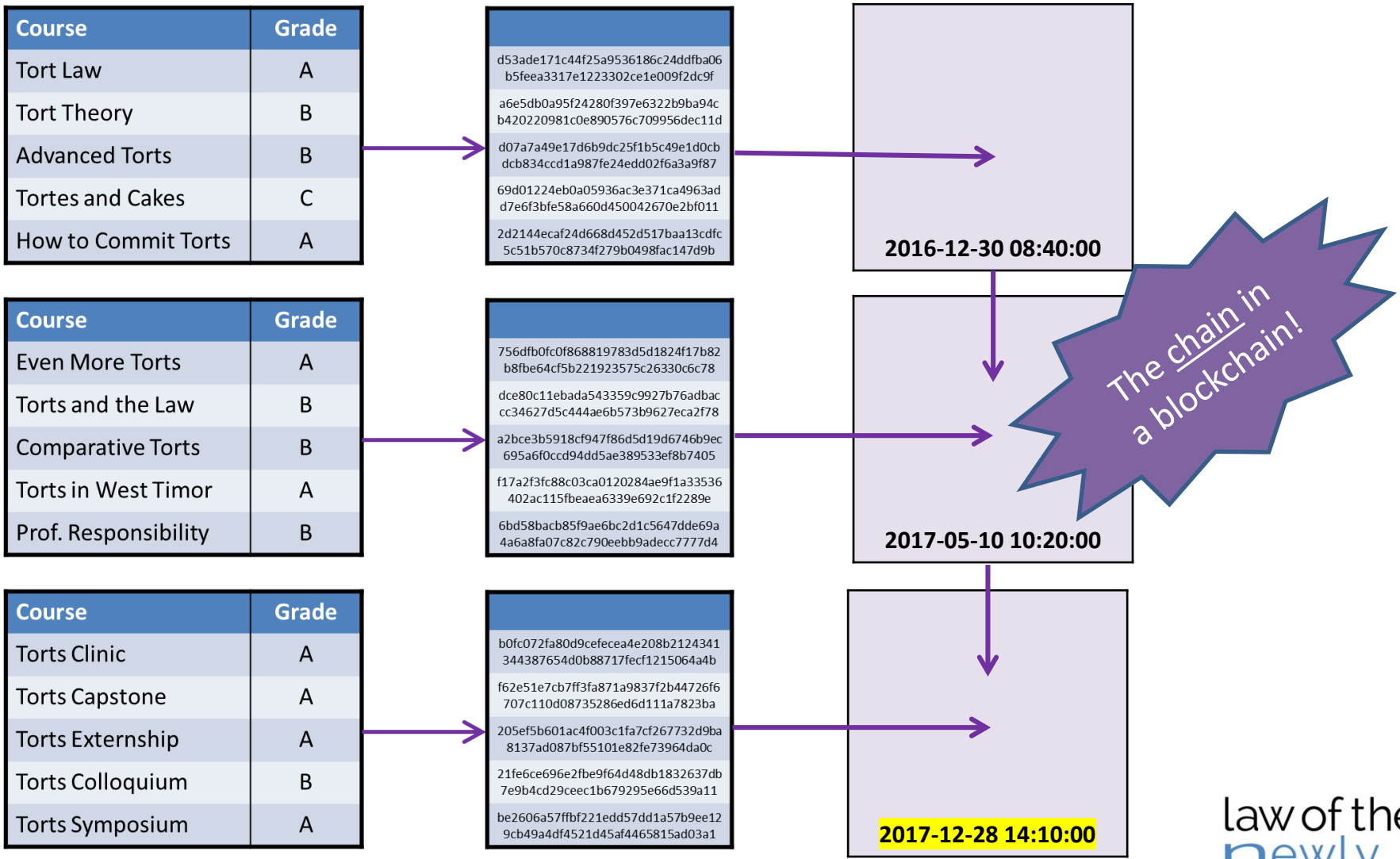
law of the newly Possible
newlypossible.org

Refining our illustration



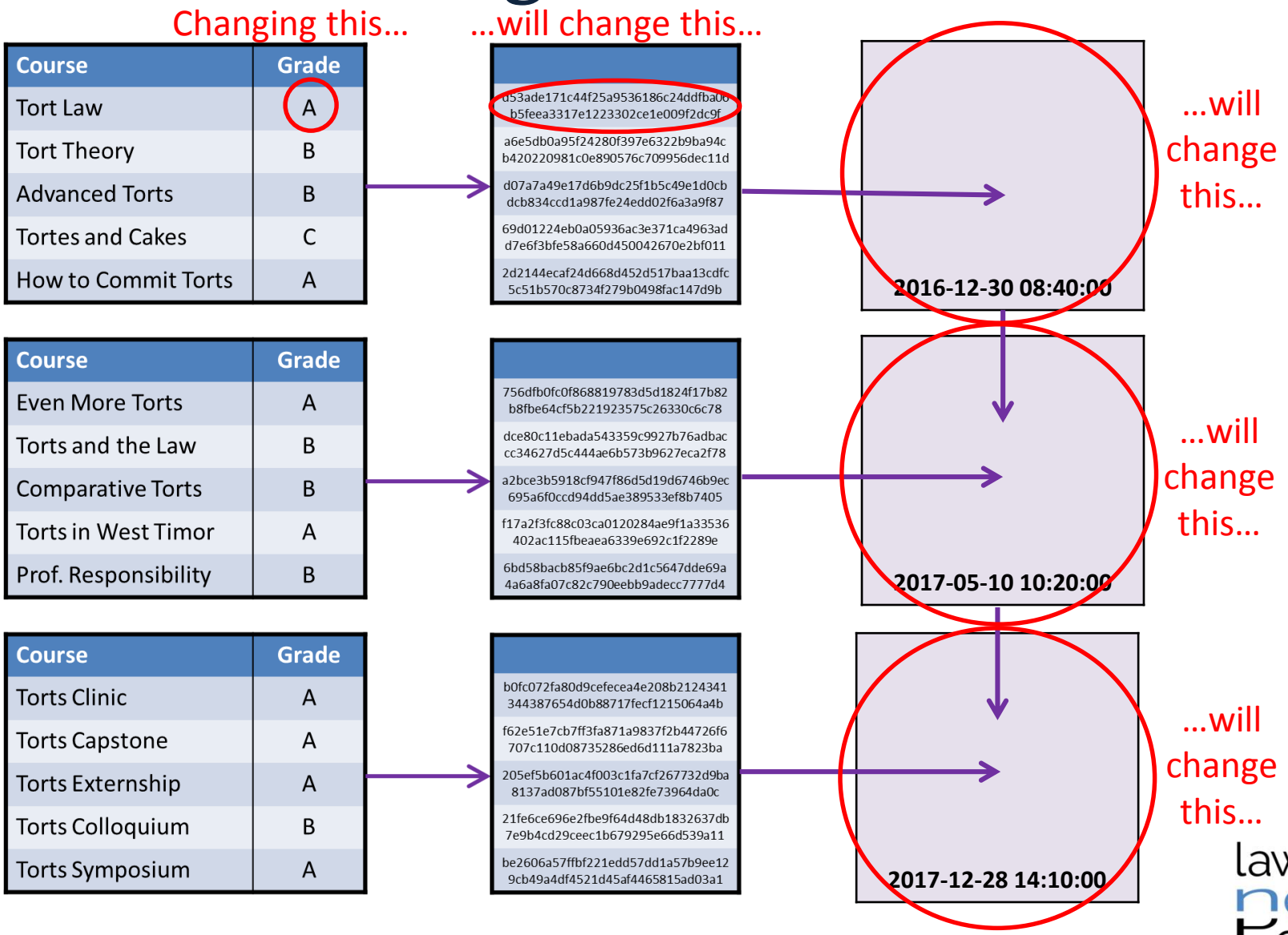
law of the newly possible
newlypossible.org

Refining our illustration



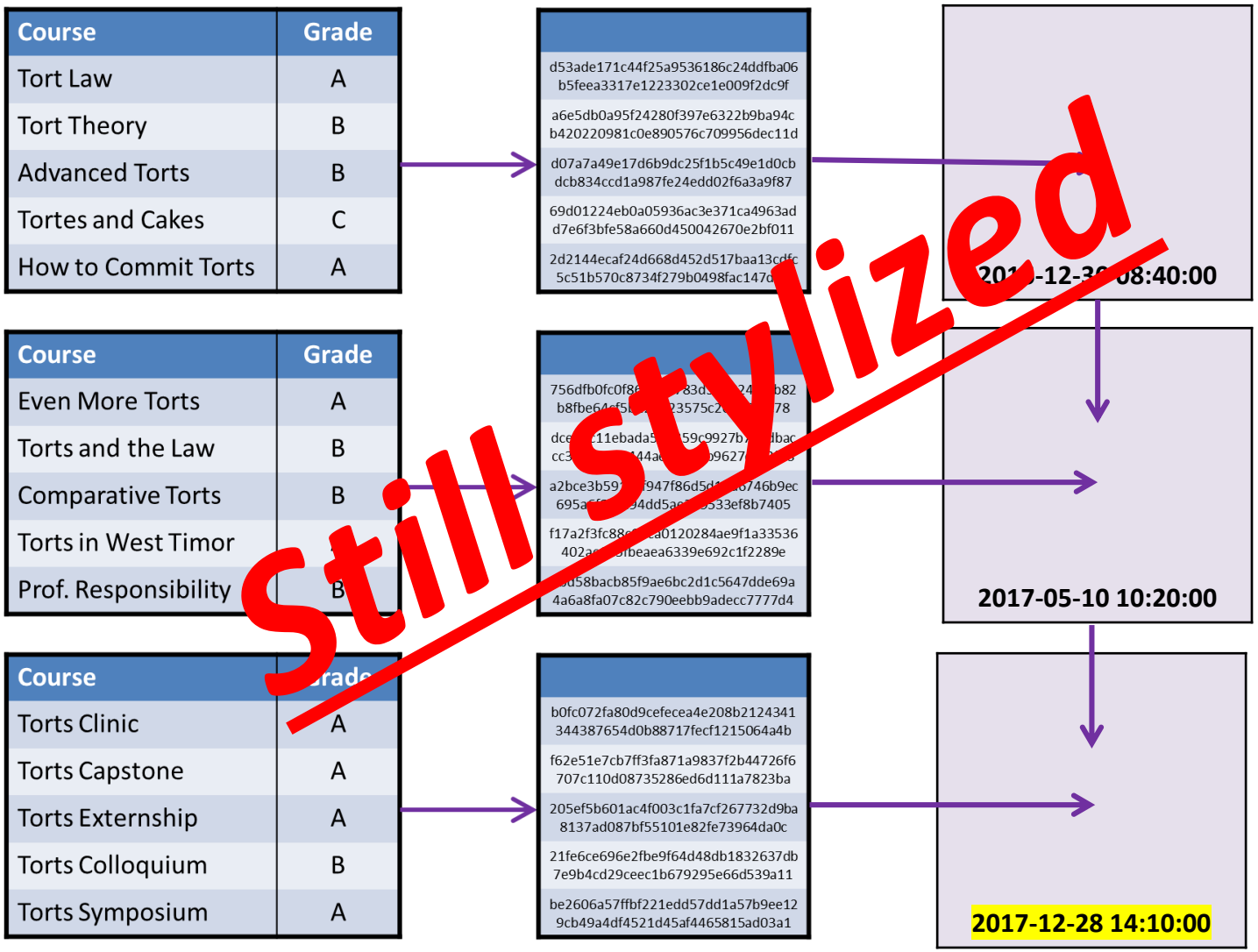
law of the newly Possible
newlypossible.org

Refining our illustration



law of the newly Possible
newlypossible.org

Refining our illustration



law of the newly Possible
newlypossible.org

Why?

- Authenticatable: Deviation is identifiable
- Decentralized: Shared among participants rather than controlled by a central authority
- Direct: Intermediaries are unnecessary

But...

- Scalable?
- Speedy?
- Robust?

And for the really crazy….

Blockchain mining!

By Xiangfu (Own work) [CC BY-SA 4.0 (https://creativecommons.org/licenses/by-sa/4.0)], via Wikimedia Commons, https://upload.wikimedia.org/wikipedia/commons/f/f4/Icarus_Bitcoin_Mining_rig.jpg
By Marco Krohn (Own work) [CC BY-SA 4.0 (https://creativecommons.org/licenses/by-sa/4.0)], via Wikimedia Commons, https://upload.wikimedia.org/wikipedia/commons/3/37/Cryptocurrency_Mining_Farm.jpg

Some early and potential uses

- Cryptocurrencies (including the original Bitcoin)
- Personal Identification
- Property registration
- Software verification
- “Smart” contracts
- Medical records
- Voting
- …!