Blockchain Education as a Public Good

Funding the Commons 2022

Kate Sills

@kate_sills

1.

The Problem

Isn’t it just a bunch of scams?

Right on! I actually just put all of my retirement savings in [scam]!

The Knowledge Problem

- People are unable to evaluate blockchain projects.
- Good projects are unfairly maligned if everything seems equally risky or scammy.

2.

Blockchain Education is a Public Good

Blockchain Education is a Public Good

Difficulty of excluding potential beneficiaries	Subtractability of Use: High	Subtractability of Use: Low
High	**Common-pool resources**: groundwater, lakes, forests	**Public goods**: national defense, knowledge, fire protection
Low	**Private Goods**: food, clothing, automobiles	**Toll goods**: theatres, private clubs

Ostrom, Elinor. 2010. "Beyond Markets and States: Polycentric Governance of Complex Economic Systems." American Economic Review, 100 (3): 641-72.

3.

Effective education is understanding & correcting a student's already existing mental model

Traditional education: knowledge transfer

Actually, We Construct Mental Models

- May be contradictory
- May be incomplete
- May be confused with similar things
- May be used as a heuristic to save time thinking

Redish, Edward F. "Implications of cognitive studies for teaching physics." American Journal of Physics 62.9 (1994): 796-803.

How to change someone's mind

The proposed replacement model must be:

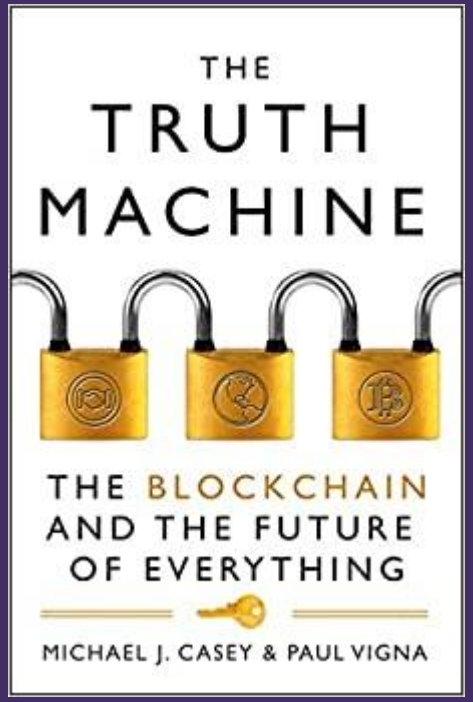
- understandable
- plausible
- seen as useful

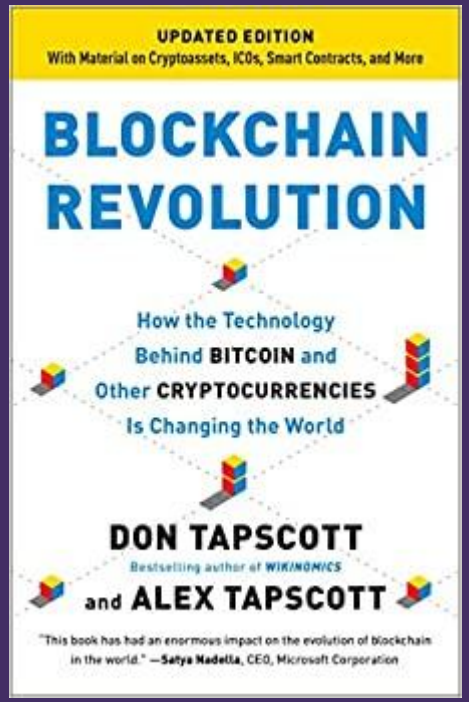
There must be a **strong conflict** with predictions based on the existing model.

Redish, Edward F. "Implications of cognitive studies for teaching physics." American Journal of Physics 62.9 (1994): 796-803.

4.

Blockchain Mental Models


THE
TRUTH
MACHINE
THE BLOCKCHAIN
AND THE FUTURE
OF EVERYTHING
MICHAEL J. CASEY & PAUL VIGNA


UPDATED EDITION
With Material on Cryptoassets, ICOs, Smart Contracts, and More
BLOCKCHAIN
REVOLUTION
How the Technology
Behind BITCOIN and
Other CRYPTOCURRENCIES
Is Changing the World
DON TAPSCOTT
Bestselling author of WIKINOMICS
and ALEX TAPSCOTT
"This book has had an enormous impact on the evolution of blockchain in the world." —Satya Nadella, CEO, Microsoft Corporation

"A masterpiece. Gracefully dissects the potential of blockchain technology to take on today's most pressing global challenges."

—Hernando De Soto, Economist and President, Institute for Liberty and Democracy, Peru

"The blockchain is to trust as the Internet is to information. Like the original Internet, blockchain has potential to transform everything. Read this book and you will understand."

—Joichi Ito, Director, MIT Media Lab

"In this extraordinary journey to the frontiers of finance, the Tapscotts shed new light on the blockchain phenomenon and make a compelling case for why we all need to better understand its power and potential."

—Dave McKay, President and CEO, Royal Bank of Canada

"Deconstructs the promise and peril of the blockchain in a way that is at once accessible and erudite. *Blockchain Revolution* gives readers a privileged sneak peak at the future."

—Alec Ross, author, *The Industries of the Future*

"If ever there was a topic for demystification, blockchain is it. Together, the Tapscotts have achieved this comprehensively and in doing so have captured the excitement, the potential, and the importance of this topic to everyone."

—Blythe Masters, CEO, Digital Asset Holdings

"This is a book with the predictive quality of Orwell's *1984* and It's quite a ride."

—Yochai Benkler, Berkman Professor of Entrepreneurial Legal Studies, Harvard Law School

"If you work in business or government, you need to understand the blockchain revolution. No one has written a more thoroughly researched or engaging book on this topic than Tapscott and Tapscott."

—Erik Brynjolfsson, Professor at MIT; coauthor of *The Second Machine Age*

"An indispensable and up-to-the-minute account of how the technology underlying bitcoin could—and should—unleash the true potential of a digital economy for distributed prosperity."

—Douglas Rushkoff, author of *Present Shock* and *Throwing Rocks at the Google Bus*

"Technological change that used to develop over a generation now hits us in a relative blink of the eye, and no one tells this story better than the Tapscotts."

—Eric Spiegel, President and CEO, Siemens USA

"Few leaders push us to look around corners the way Don Tapscott does. With *Blockchain Revolution* he and his son Alex teach us, challenge us, and show us an entirely new way to think about the future."

—Bill McDermott, CEO, SAP SE

—an invention that in time may prove as momentous as the invention of printing."

—James Rickards, author of *Currency Wars* and *The Death of Money*

"*Blockchain Revolution* serves as an atlas to the world of digital money, masterfully explaining the current landscape while simultaneously illuminating a path forward toward a more equitable, efficient, and connected global financial system."

—Jim Breyer, CEO, Breyer Capital

"*Blockchain Revolution* is the indispensable and definitive guide to this world-changing technology."

—Jerry Brito, Executive Director, Coin Center

"Incredible. Really incredible. The Tapscotts' examination of the blockchain as a model for inclusion in an increasingly centralized world is both nuanced and extraordinary."

—Steve Luczo, Chairman and CEO, Seagate Technology

"Makes a powerful case for blockchain's ability to increase transparency but also ensure privacy. In the authors' words, 'The Internet of Things needs a Ledger of Things.'"

—Chandra Chandrasekaran, CEO and Managing Director, Tata Consultancy Services

"The epicenter of trust is about to diffuse! The definitive narrative on the revolutionary possibilities of a decentralized trust system."

—Frank D'Souza, CEO, Cognizant

policy maker needs to read *Blockchain Revolution*."

—Brian Fetherstonhaugh, Chairman and CEO, OgilvyOne Worldwide

"*Blockchain Revolution* sets the table for a wave of technological advancement that is only just beginning."

—Frank Brown, Managing Director and Chief Operating Office, General Atlantic

"A must read. You'll gain a deep understanding of why the blockchain is quickly becoming one of the most important emerging technologies since the Internet."

—Brian Forde, Director of Digital Currency Initiative, MIT Media Lab

"Blockchain technology has the potential to revolutionize industry, finance, and government—a must read for anyone interested in the future of money and humanity."

—Perianne Boring, Founder and President, Chamber of Digital Commerce

"When generational technology changes the world in which we live, we are truly fortunate to have cartographers like Don Tapscott, and now his son Alex, to explain where we're going."

—Ray Lane, Managing Partner, GreatPoint Ventures; Partner Emeritus, Kleiner Perkins

"Don and Alex have written the definitive guidebook for those trying to navigate this new and promising frontier."

—Benjamin Lawsky, Former Superintendent of Financial Services, State of New York; CEO of The Lawsky Group

Digital Signatures (1977)

Signing

Create a random number. That’s your private key. It should be kept secret.

Now you can sign messages, creating a digital signature, which is unforgeable. No one else can create this digital signature - only you can.

Digital Signatures (1977)

Digital signatures


```
0x3045022100e16236fc16c6a3cd
5df8c47597f27a852f54b5c8f5cb
4a1c18c215d48715a54002207868
db852cf8c11c7c09086164fc0d8d
754e46ddc50eb3fcf458c4cd6d9e
da8d
```

Digital Signatures (1977)

Verifying a signature

Derive a new number from your private key. You can share this one publicly - let’s call it a public key.

With the public key, someone else can verify that your signature is valid for that particular message.

Digital Signatures (1977)

Digital signatures do not encrypt

Think of it as a stamp on a document.

Nothing about the document is hidden.

Digital Signatures (1977)

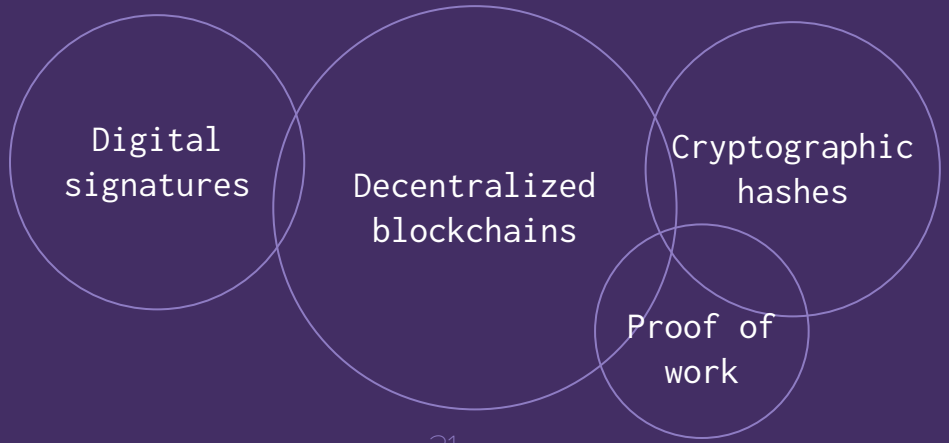
Signed messages are tamper-evident

Because a signature is only valid for a particular message, if that message changes at all - that signature is invalid.

Digital Signatures (1977)

Digital signatures don’t require a blockchain.

Blockchains like Bitcoin make extensive use of digital signatures, but digital signatures existed long before Bitcoin.



Digital Signatures (1977)

How blockchains use digital signatures

When you sign and submit a transaction to a blockchain, you’re creating a digitally signed message with your private key.

“We needn’t worry about weak firewalls, thieving employees, or insurance hackers. If we’re both using bitcoin, if we can store and exchange bitcoin securely, then we can store and exchange highly confidential information and digital assets securely on the blockchain.”

Blockchain Revolution, page 40

Mental Model

✓ Bitcoin is secure

✗ We can store highly confidential information on “the blockchain”

“...one of the most important non-currency applications of Bitcoin’s blockchain could be security itself.”

The Truth Machine, page 42

Mental Model

✓ Bitcoin is secure

✗ We can store highly confidential information on “the blockchain”

✗ Blockchains protect against hacks that reveal private data

“...the blockchain is encrypted: it uses heavy-duty encryption involving public and private keys...”

Blockchain Revolution, page 6

Mental Model

✓ Bitcoin is secure

✗ We can store highly confidential information on “the blockchain”

✗ Blockchains protect against hacks that reveal private data

✗ Bitcoin is encrypted

✓ Blockchains involve public and private keys

“it uses heavy-duty encryption involving public and private keys (rather like the two-key system to access a safety deposit box)”

Blockchain Revolution, page 6


30-07
30-07

Mental Model

✓ Bitcoin is secure

✗ We can store highly confidential information on “the blockchain”

✗ Blockchains protect against hacks that reveal private data

✗ Bitcoin is encrypted

✓ Blockchains involve public and private keys

✗ A public and private key pair is like the two keys of a safety deposit box

“When the user ‘signs’ their public key with their private key, that action mathematically proves to outsiders that the user has control of the underlying information and can then assign, or send it, to another person’s public key.”

The Truth Machine, page 64

“The concept of a ‘signature’ in cryptography means something far more scientific than a handwritten scrawl; it entails combining two associated numbers, or “keys”–one publicly known, the other private–to mathematically prove that the entity making the signature is uniquely authorized to do so.”

The Truth Machine, page 30

Mental Model

✓ Bitcoin is secure

✗ We can store highly confidential information on “the blockchain”

✗ Blockchains protect against hacks that reveal private data

✗ Bitcoin is encrypted

✓ Blockchains involve public and private keys

✗ A public and private key pair is like the two keys of a safety deposit box

✗ The two keys are combined somehow to prove ownership

✗ The private key is used to sign the public key

“If all we have is a cryptographically signed certificate from some institution, we may have a reliably certified document, but we’re also vulnerable to that institution’s unilateral power to revoke its signature. This is effectively what President Trump has done in reversing some of the orders of his predecessors–in revoking the rights of transgender soldiers, for example. The same risks always apply with digitally signed rights when they don’t reside in an immutable record”

The Truth Machine, page 218

“Note the deliberate choice of the most secure, permissionless blockchain, Bitcoin’s. [In a permissioned blockchain], the central authority controlling the network could always override the public keys of the individual and could revoke their educational certificates.”

The Truth Machine, page 219

Mental Model

✓ Bitcoin is secure

✗ We can store highly confidential information on “the blockchain”

✗ Blockchains protect against hacks that reveal private data

✗ Bitcoin is encrypted

✓ Blockchains involve public and private keys

✗ A public and private key pair is like the two keys of a safety deposit box

✗ The two keys are combined somehow to prove ownership

✗ The private key is used to sign the public key

✗ Digital signatures can be made invalid afterward by the signer

✗ The signed message can be tampered with, without anyone knowing

✗ Control of a blockchain allows you to control private keys/signatures

More incorrect ideas

Some more examples:

- Blockchain consensus produces truth
- By providing a solution to the “double-spend problem,” blockchains can guarantee the uniqueness of assets generally

5.

How to fix wrong ideas

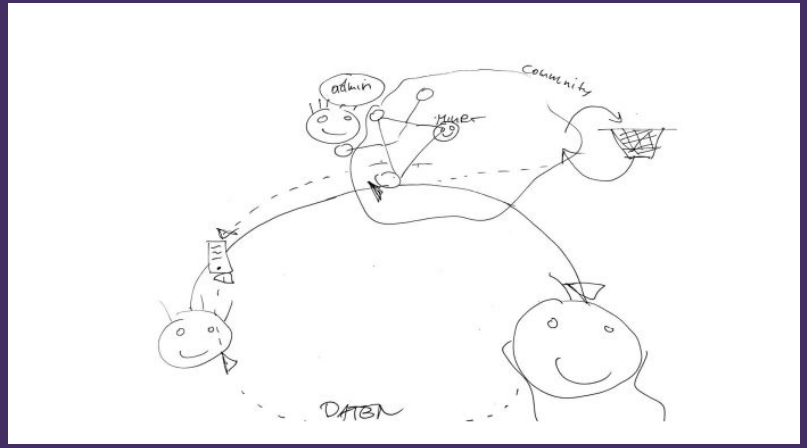
How can we fix wrong ideas?

1. Understand the audience's particular mental model. Everyone has their own, unique version.
2. Convey the correct mental model
3. To replace someone's mental model, "there must be a strong conflict with predictions based on the existing model."
    a. Tell them something true that contradicts their current model
    b. Tell them something surprising

How can we fix wrong ideas?

User Studies

Mai, Alexandra, et al. "User mental models of cryptocurrency systems-a grounded theory approach." Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020). 2020.



Create Surprising Products

Products that Break People's Brains

E.g. POAP but entirely off-chain

An event organizer uses their private key to sign a claim that the attendee attended the event.

This produces a signature that can be verified by anyone who knows the public key of the organizer.

Creates conflicts:

- No blockchain, but we get a tamper-evident document if we store the signature.
- Uses public/private keys, but not encrypted.

Products that Break People's Brains

While knowledge is a public good, we can create products that aren't! They are excludable and therefore profitable (e.g. pay $5 to make a badge without a watermark).

Going against the common mental model might indicate a market opportunity.

Thanks!

Any questions?

You can find me at @kate_sills & katelynsills@gmail.com