Cryptography & Law

an Unexpected Encounter that was Obvious all Along

Prof. Aggelos Kiayias
www.kiayias.com

aggelos.kiayias@ed.ac.uk

gratefully acknowledging the support of the European Research Council - Starting Grant CODAMODA

Law

- Regulates interactions between *persons* ensuring fairness, and basic rights.

- In this way, law protects *persons* from other *persons* with conflicting interests.

- Protection is achieved by relying on rule of law and social institutions.

Cryptography

- is the science of communicating secret messages in the presence of an adversary.

Modern Cryptography

- is the science of redistributing trust in any system that emerges from the interaction of multiple *persons*.

- In this way, cryptography protects *persons* from other *persons* with conflicting interests.

- Protection is achieved by relying on hard mathematical problems.

Case study : Money

- What is money?

Properties of Money

- a medium of exchange

can be used as medium for the exchange of goods - no barter

- a unit of account

can be used for pricing of all goods and services, for accounting purposes and debt recording.

- a store of value

storing and retrieving it at a point in the future maintains its value.

Creating Money

Money 1.0 : using a trusted object

Analysis of Money 1.0

- a medium of exchange
- a unit of account
- a store of value

mediocre
[ok for face to face transactions]

mediocre fungible, but not divisible well. it might be forgeable.

bad. some objects may deteriorate, others may have unknown hidden quantities.

Creating Money

Money 2.0 : using a trusted entity

Trusted entity issues “IOU”s

Analysis of Money 2.0

- a medium of exchange
- a unit of account
- a store of value

good
[for transactions within the domain of the trusted entity]

great!
fungible & divisible.

mediocre
[tied to the availability & reputation of the issuing entity]

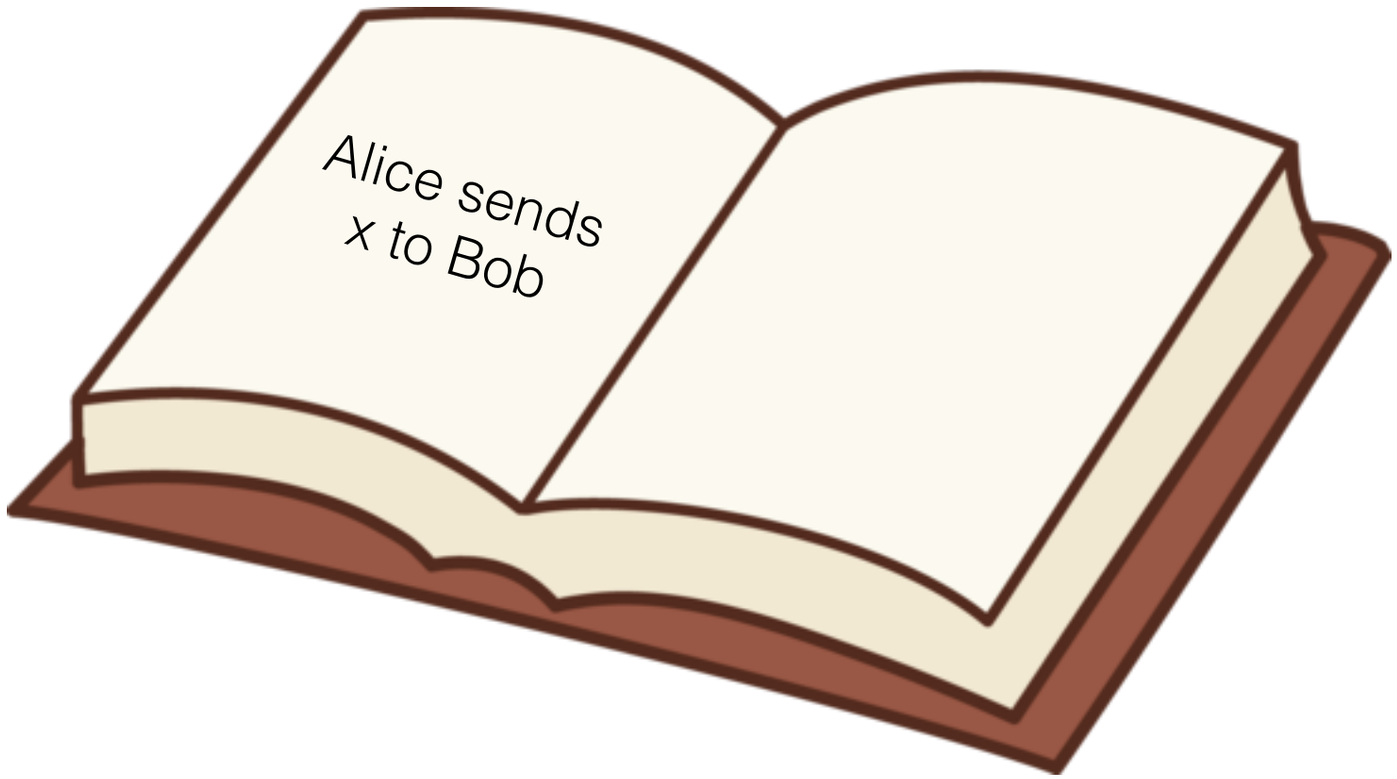
Creating Money

Money 3.0 : Bitcoin

Enter Blockchain & distributed Ledgers

The never-ending book parable

A “book” of transactions

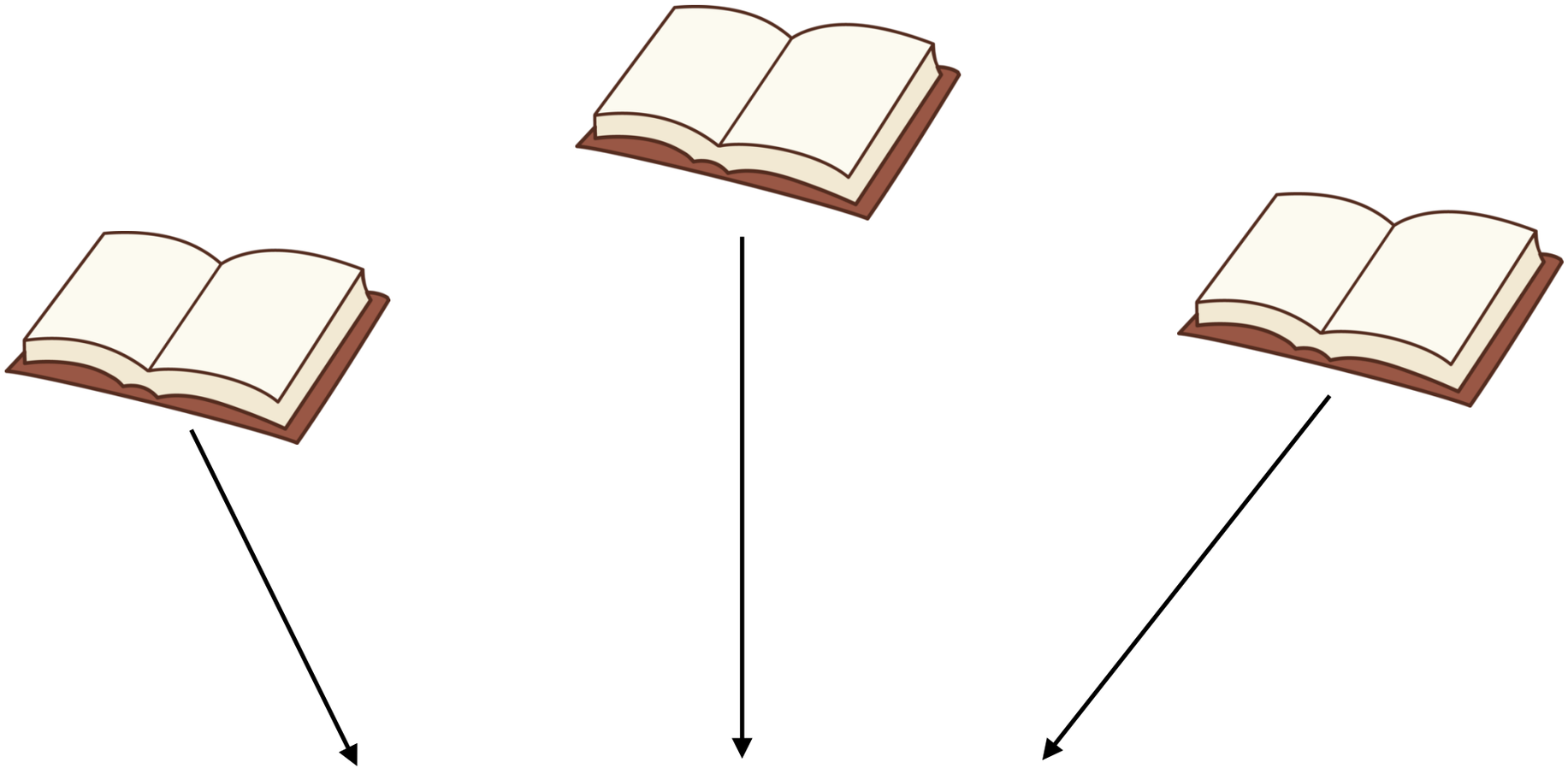


- Each new page requires some effort to produce.
- Anyone can be a scribe and produce a page.
- New pages are produced indefinitely as long as scribes are interested in doing so.

Importance of Consensus

- If multiple conflicting books exist, which is the “right one”?

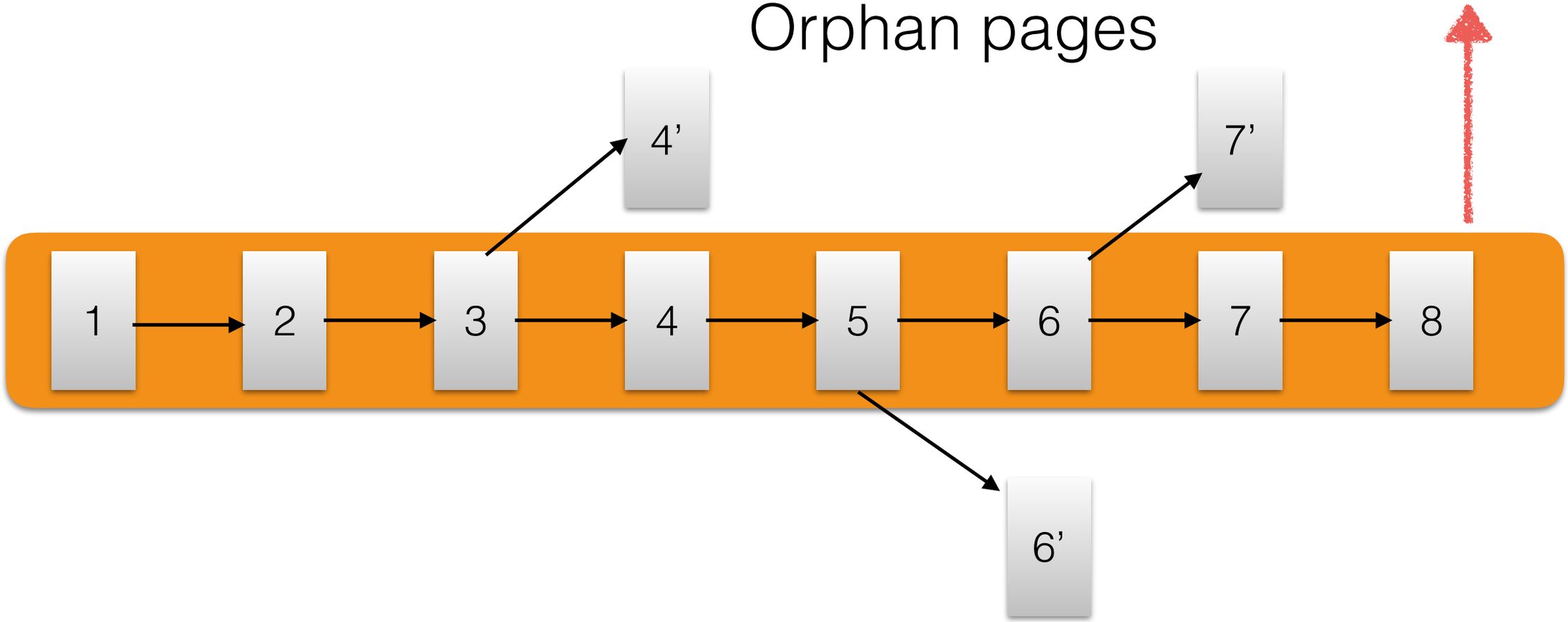
Choosing the correct book



The **current book** to work on & refer to is the book with the most pages. if multiple exist, just pick one at random.

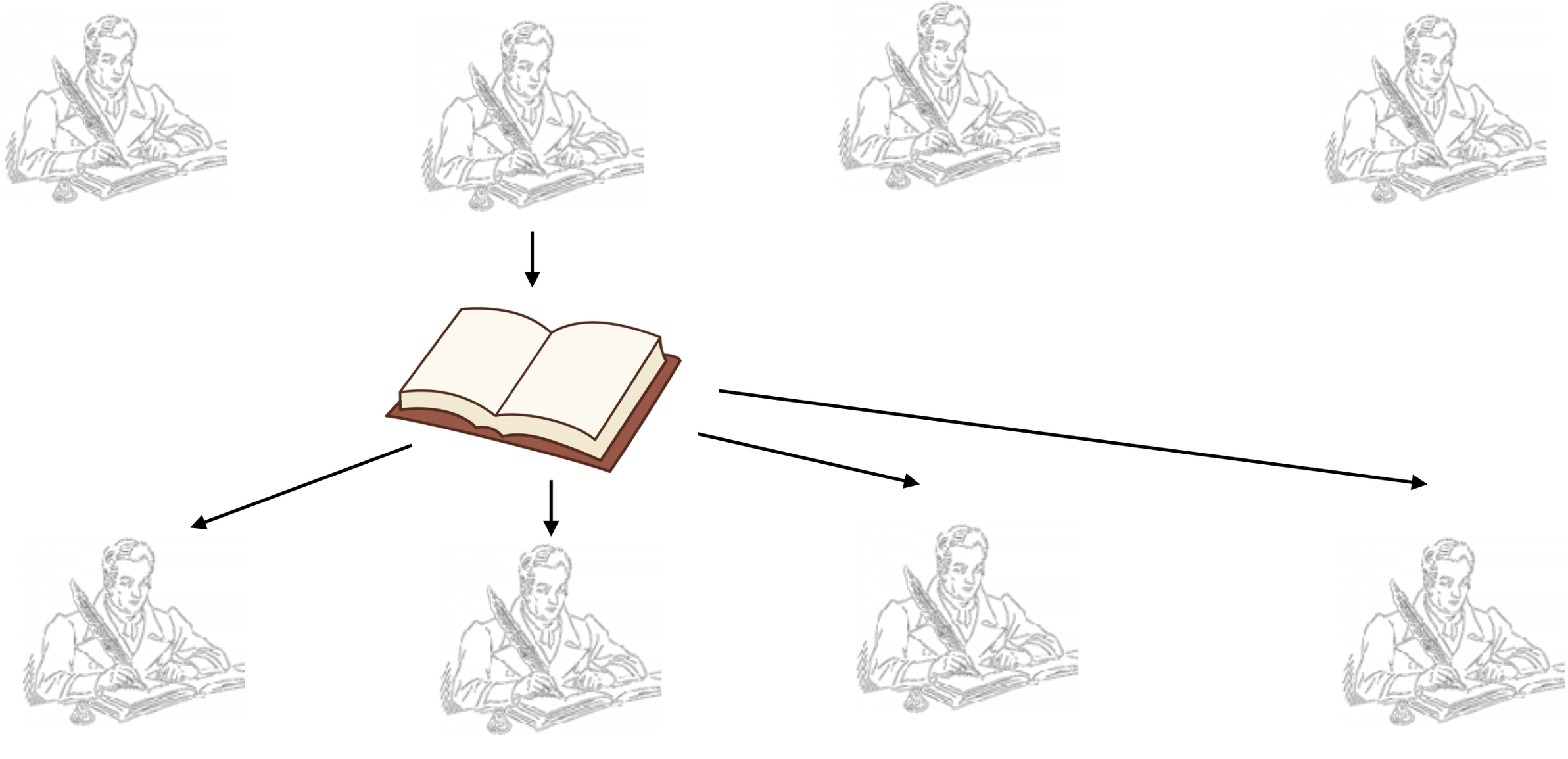
Assembling the current book

Current version of the book:



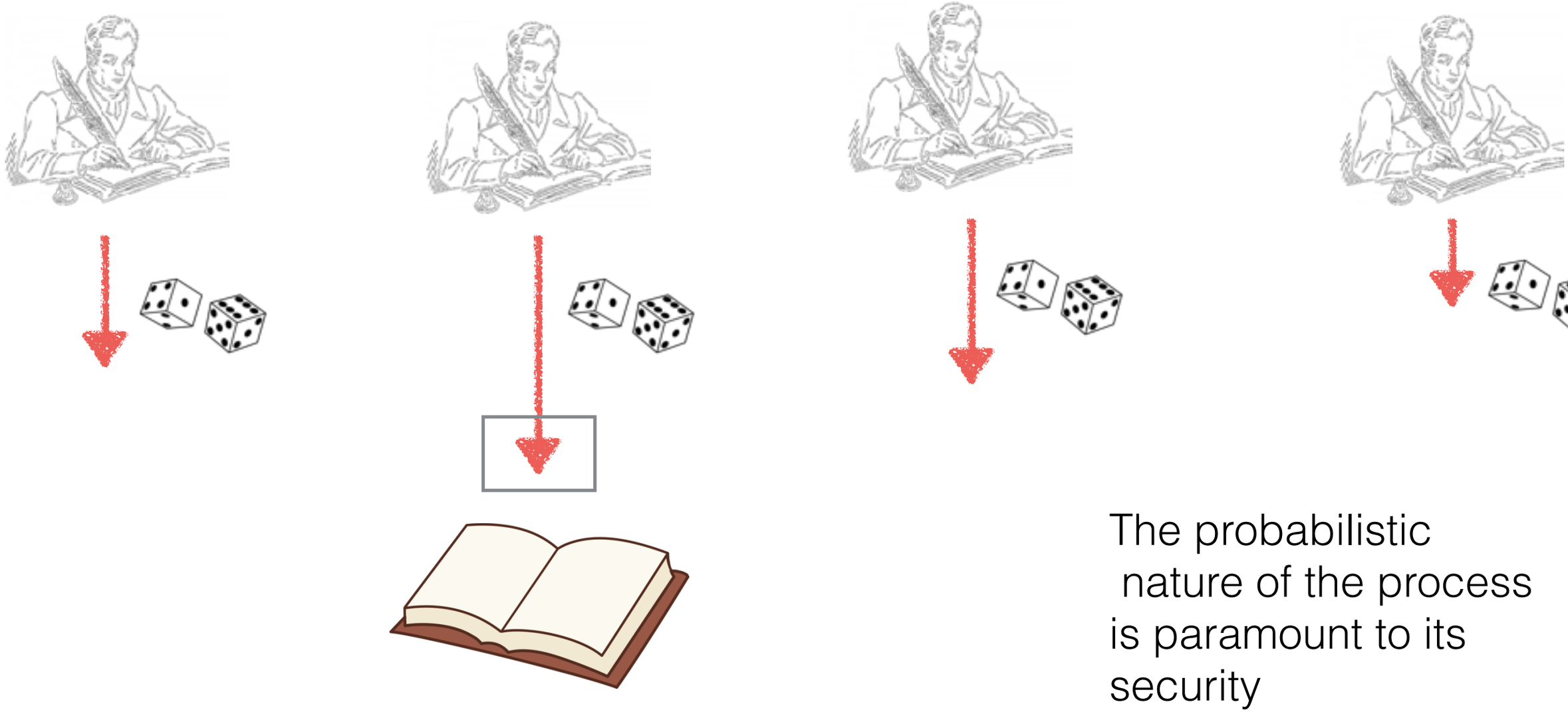
Rules of extending the book

The first scribe that discovers
a page announces it to everyone else



Effort is needed to produce a page

equivalent to : each page needs a special combination from a set of dice to be rolled.



The probabilistic nature of the process is paramount to its security

The benefits of randomness

Imagine two scribes  working together

Unlikely
to continuously
be lucky
together

eventually
one book
will be longer
and be adopted
by both of them

Being a scribe

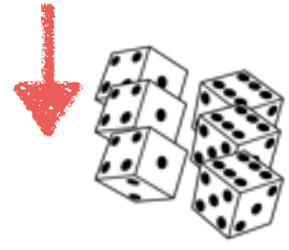
- Anyone can be a scribe for the book.
- As long as you have a set of dice.
- The more dice one has, the higher the likelihood to produce the winning combination to make a page.

Multiple scribes and probability of page extension

10%

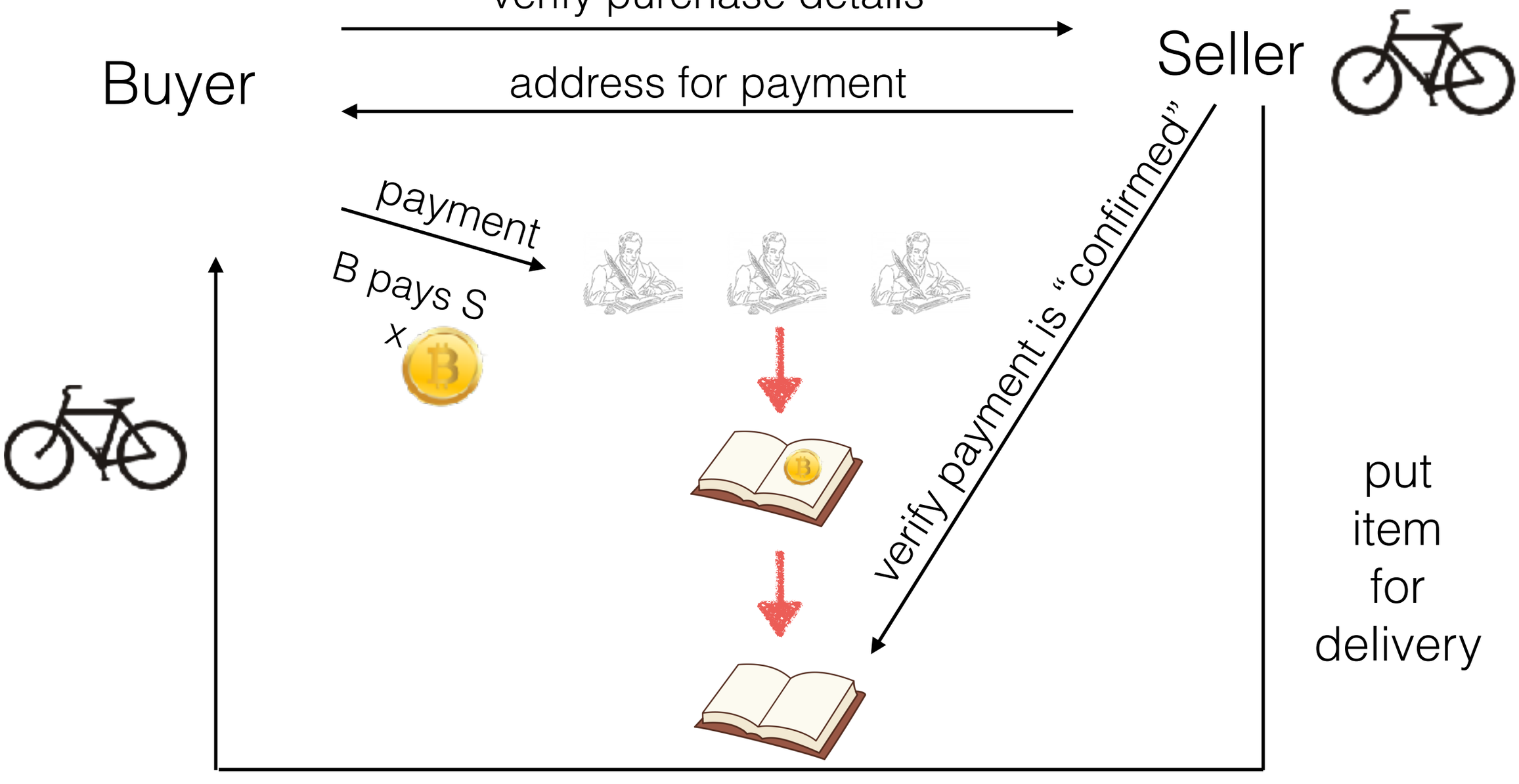
20%

40%



30%

Using the book - Money 3.0



Can one rewrite the book?

the more pages pile up on top of a page, the less likely it is, to have the page removed from the book

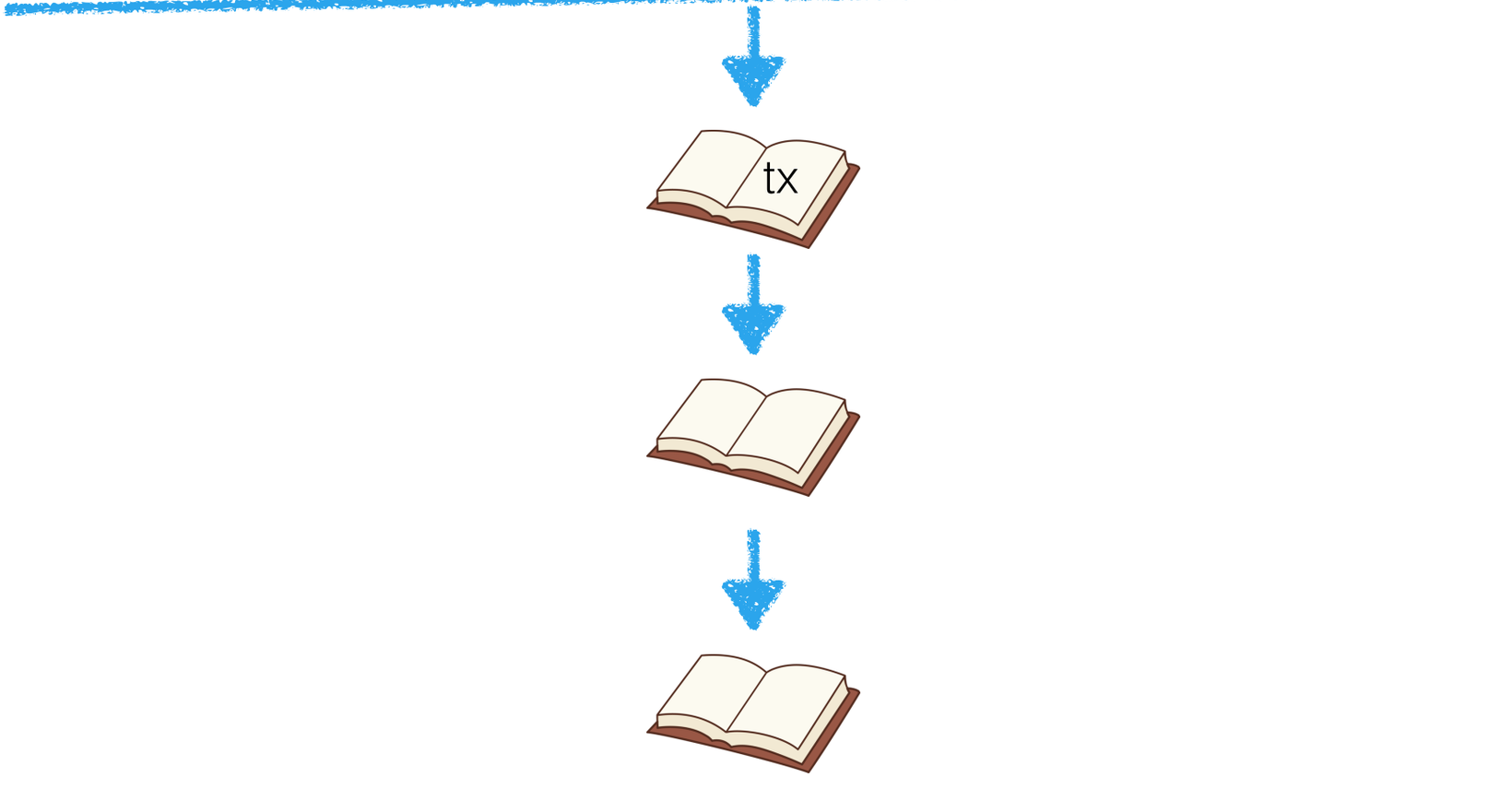
Rewriting the book

10%

20%

40%

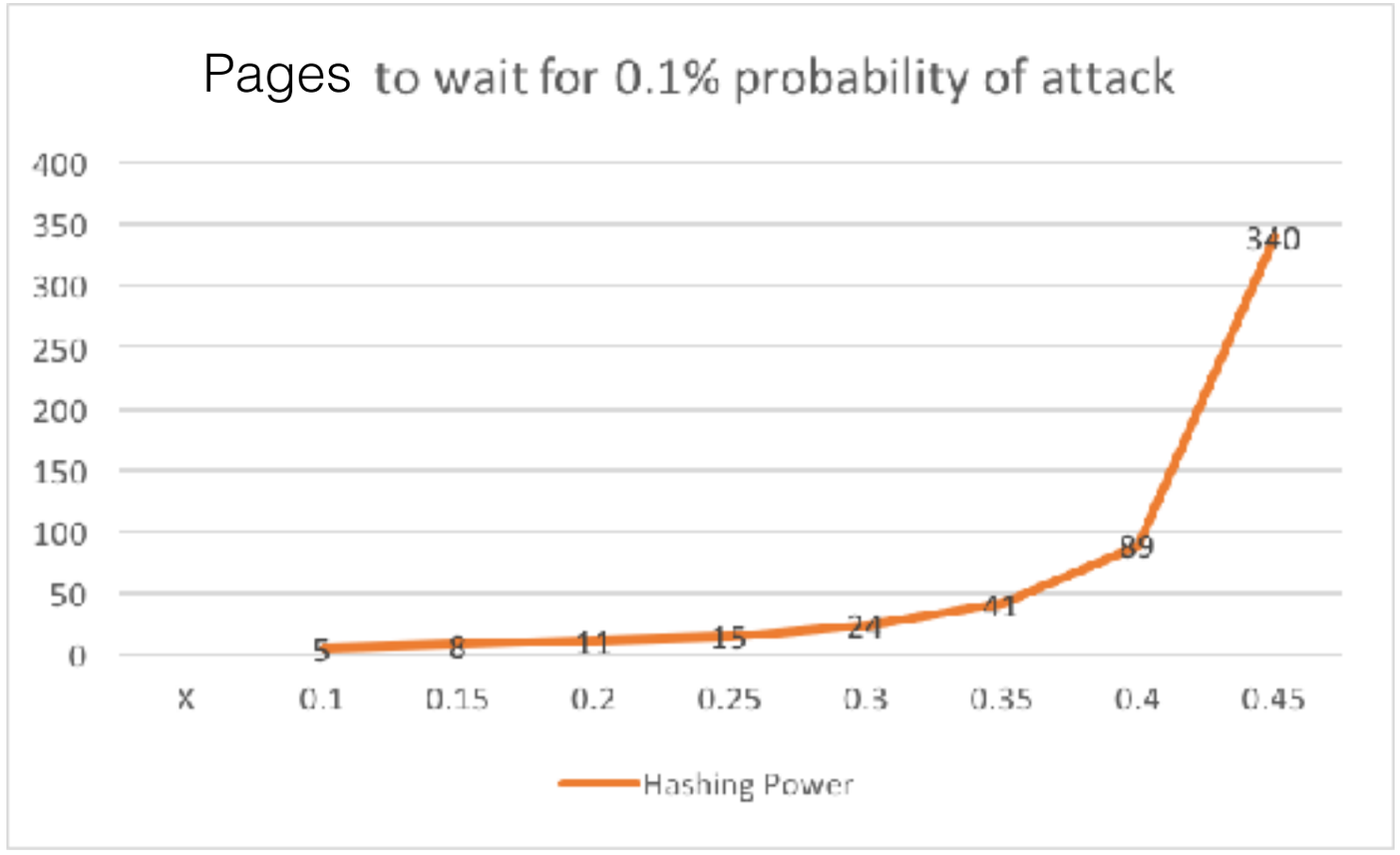
30%



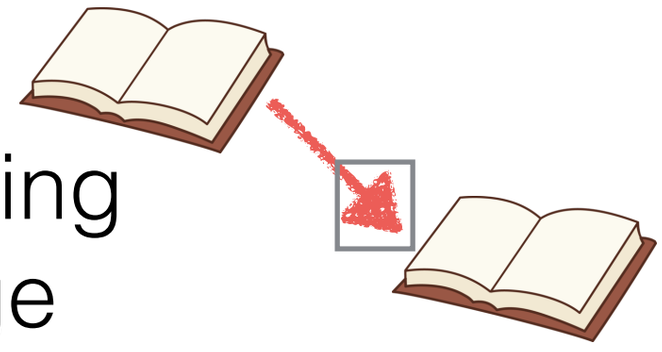
Rewriting the book, 2

- The probability of rewriting the book can be made arbitrarily small as long as one waits for enough pages.

```
P < 0.001
    q=0.10    z=5
    q=0.15    z=8
    q=0.20    z=11
    q=0.25    z=15
    q=0.30    z=24
    q=0.35    z=41
    q=0.40    z=89
    q=0.45    z=340
```



Parable & Reality

book 	the “blockchain”
scribe 	“Miners” / Computer systems that organize transactions in blocks
producing a page 	Solving a **cryptographic puzzle** that is **moderately hard** to solve
rolling a set of dice 	Using a computer to test for a solution from a large space of candidates solutions

Analysis of Money 3.0

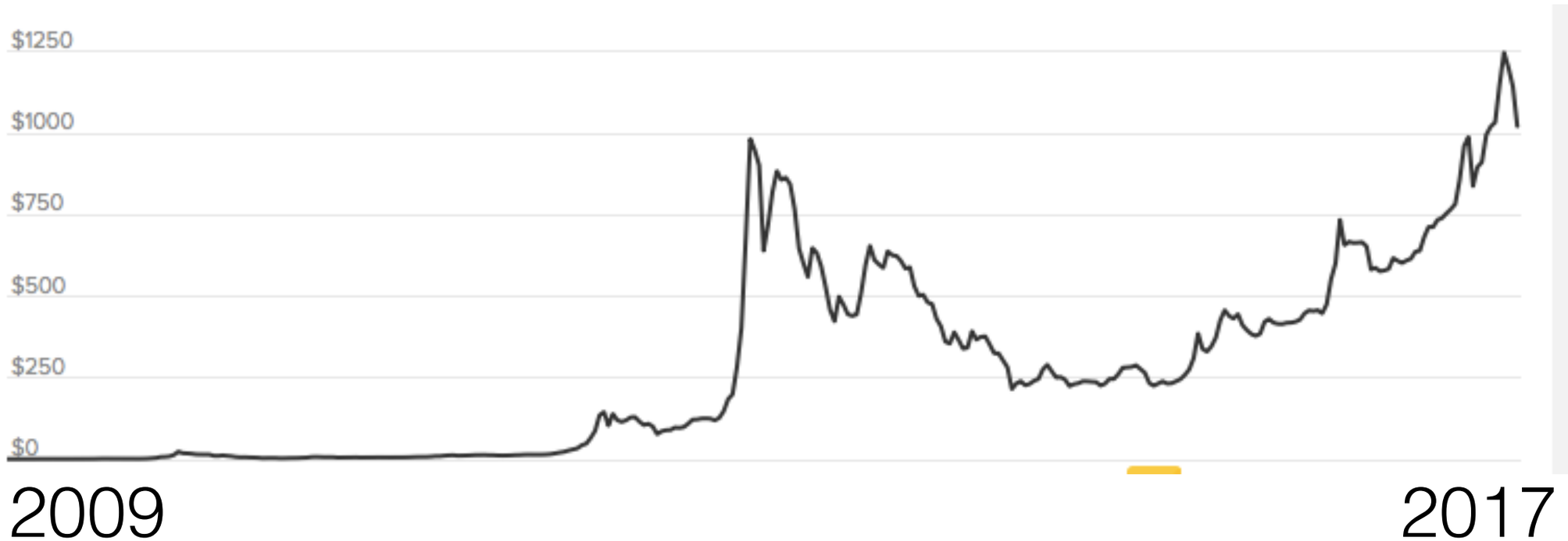
- a medium of exchange
- a unit of account
- a store of value

improving
[assuming internet connectivity / adoption]

great!
fungible & divisible.

good
[no trusted parties - no natural deterioration]

Bitcoin price



Careful : just because something works it does not mean it will be used!

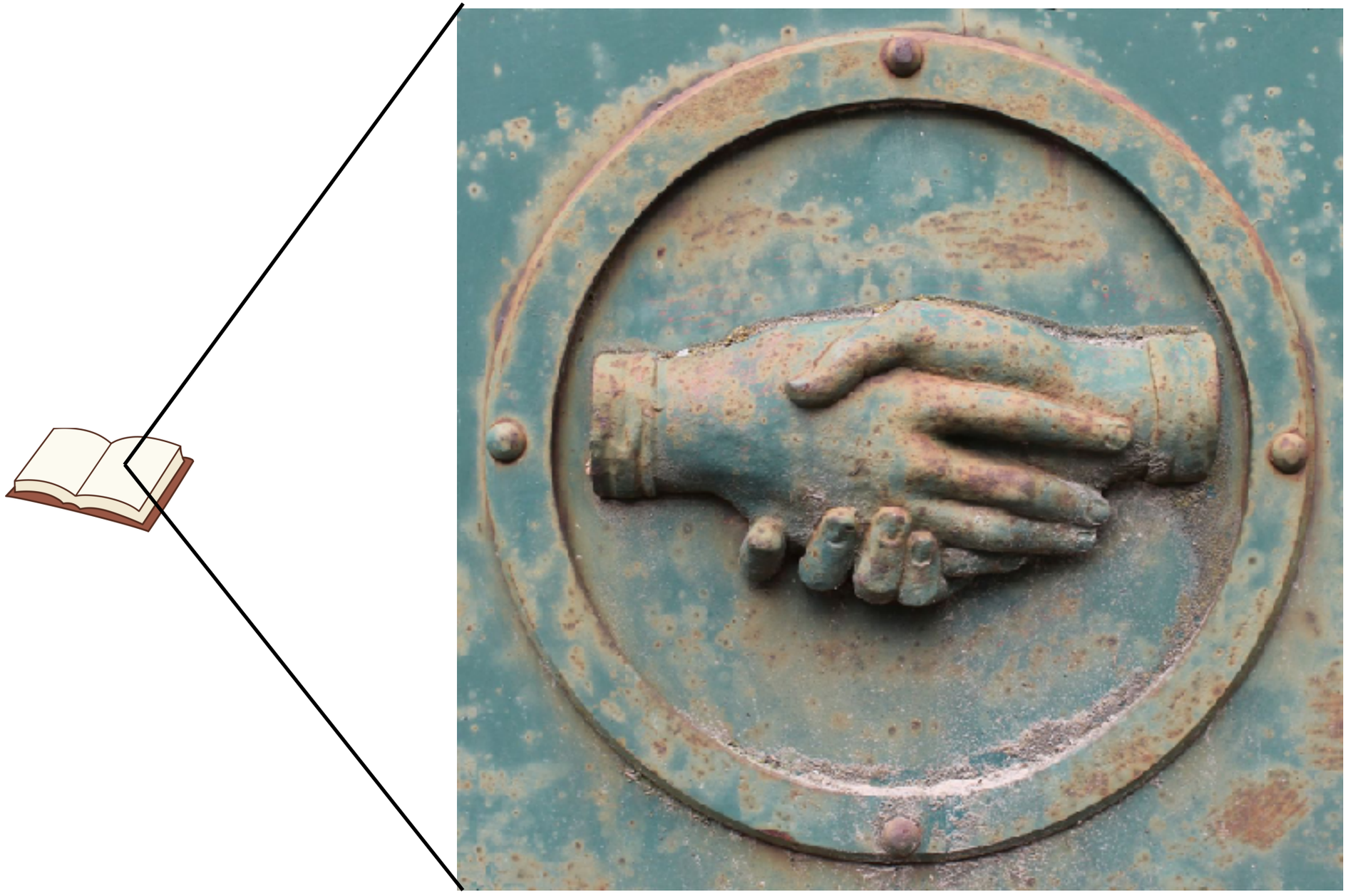
From Money to Smart Contracts

- Since we have created **the book**, why stop at recording monetary transactions?

- We can encode in the book's pages **arbitrary relations** between persons.

- Furthermore, scribes, can perform tasks such as verifying that stakeholders **comply** to contractual obligations … and **take action** if they do not.

Smart Contract



Smart Contract Operation

- A smart contract is a **piece of code** written in a formal language that records all terms for a certain engagement between a set of persons, “stakeholders.”
- Stakeholders are identified by their **accounts**.
- The smart contract has a **public state**.
- The smart contract **self executes** each time a certain trigger condition is fulfilled.

Application : The Sugarman Problem in Intellectual Property

- Sixto Rodriguez 70's music albums never succeeded in native US
- With little to moderate success as an artist, he worked in construction
- Unbeknownst to him, his music was a big success in South Africa

Watch : *searching for sugarman* (2015) documentary.

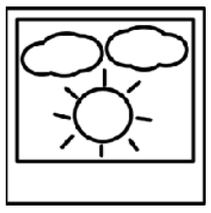
Example of Smart Contract for IP Management

receives payment

creates smart contract to manage licensing for the work

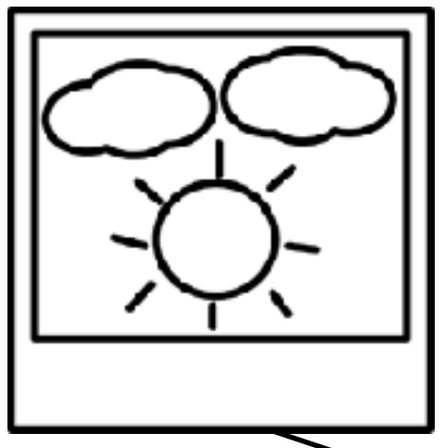
verifies licence

audits proper use of work



uses the work

Artist posts work of art



receives license

interacts with the smart contract to fulfill licensing conditions (e.g. pay)

downloads the work

SC advantages for IP management

- Beyond work & contract publication, artist can be **offline**.

- Smart contract **automatically** furnishes license and records payment.

- Royalties accrue in the blockchain and are **cryptographically secured** until claimed by the artist.

- Auditing can be made automatically and web-sites in **license violation** reported & penalized.

Take away points for IP

- Sharing is not prohibited.
- Nevertheless, royalty collection, lawful use & compliance is automatically facilitated via the smart contract.
- There is no “middle man” between artist and user.

2nd Example: Rental Agreement of Property

Owner

creates smart contract to manage rental of property

receives insurance deposit

examines request

accepts request and encodes entry key

receives payment

ok's proper exit

deposits fee + insurance deposit

receives entry key

Renter

SC Applications

- There is a multitude of other SC applications:
  - land registries.
  - financial instruments.
  - general rental / leasing agreements.
  - …

SC Challenges

- Privacy
- Efficiency of representation
- Scalability
- Verifiability & Correctness
- Expressibility

Looking into the Future

- Cryptolegal frameworks

Merging **cryptography and law** to regulate interactions of *persons* at a global scale.

Transcend geographic & **jurisdictional boundaries** to create a dynamic global social institution that **belongs to all** and can be **abused by none**.

Cryptography & Law

an Unexpected Encounter that was Obvious all Along

Prof. Aggelos Kiayias
www.kiayias.com

aggelos.kiayias@ed.ac.uk

gratefully acknowledging the support of the European Research Council - Starting Grant CODAMODA