Blockchain Mechanics to Insurance Opportunities

Stephen J. Mildenhall

April 24, 2019

ST. JOHN'S UNIVERSITY
Tobin College of Business
School of Risk Management

[Your Industry] Blockchain Opportunity Slide

[Your Industry] Blockchain Opportunity Slide

Your Business Problems

[Your Industry] Blockchain Opportunity Slide

Your Business Problems

Customer Experience

- Confusing products
- High expenses

[Your Industry] Blockchain Opportunity Slide

Your Business Problems

Customer Experience

- Confusing products
- High expenses

Your Problem 1

- _____
- _____

Your Problem 2

- _____
- _____

Your Problem 3

- _____
- _____

[Your Industry] Blockchain Opportunity Slide

Your Business Problems

Customer Experience

- Confusing products
- High expenses

Your Problem 1

- _____
- _____

Your Problem 2

- _____
- _____

Your Problem 3

- _____
- _____

Blockchain may be the Solution!

[Your Industry] Blockchain Opportunity Slide

Your Business Problems

Customer Experience
- Confusing products
- High expenses

Your Problem 1
- _____
- _____

Your Problem 2
- _____
- _____

Your Problem 3
- _____
- _____

Blockchain may be the Solution!

Blockchain delivers...
- Best customer experience
- Immutable record
- Enables collaboration
- One view of truth
- Facilitates reconciliation
- Lower costs
- Eliminates fraud
- Regulatory compliance
- Product innovation
- Quick to market
- _____
- _____

[Your Industry] Blockchain Opportunity Slide

Your Business Problems

Customer Experience
- Confusing products
- High expenses

Your Problem 1
- _____
- _____

Your Problem 2
- _____
- _____

Your Problem 3
- _____
- _____

Blockchain may be the Solution!

Blockchain delivers...
- Best customer experience
- Immutable record
- Enables collaboration
- One view of truth
- Facilitates reconciliation
- Lower costs
- Eliminates fraud
- Regulatory compliance
- Product innovation
- Quick to market
- _____
- _____

Any sufficiently advanced technology is indistinguishable from magic.

Arthur C. Clarke

Definition

Blockchains are **distributed** digital **ledgers** of **cryptographically signed transactions** that are grouped into **blocks.** Each block is **cryptographically linked** to the previous one after **validation** and undergoing a **consensus decision,** making it **tamper evident.** As new blocks are added, older blocks become more **difficult to modify.** New blocks are **replicated** across copies of the ledger within the network, and any **conflicts** are **resolved automatically** using established rules.

Blockchain Technology Overview, Yaga et al (2018), NIST

Description

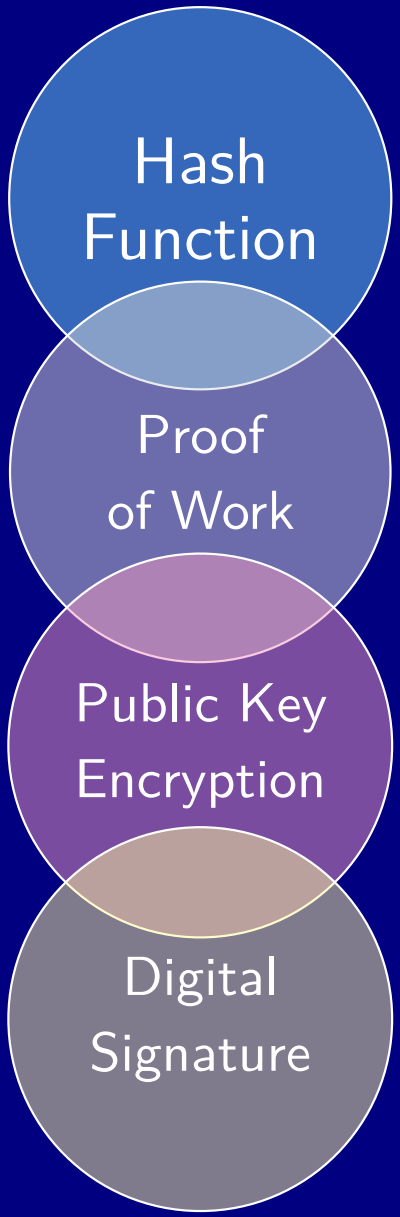
Components

- Distributed database
- Ledger
- Cryptographically...
- ...Signed transactions
- ...Linked (chained)
- Consensus Validation

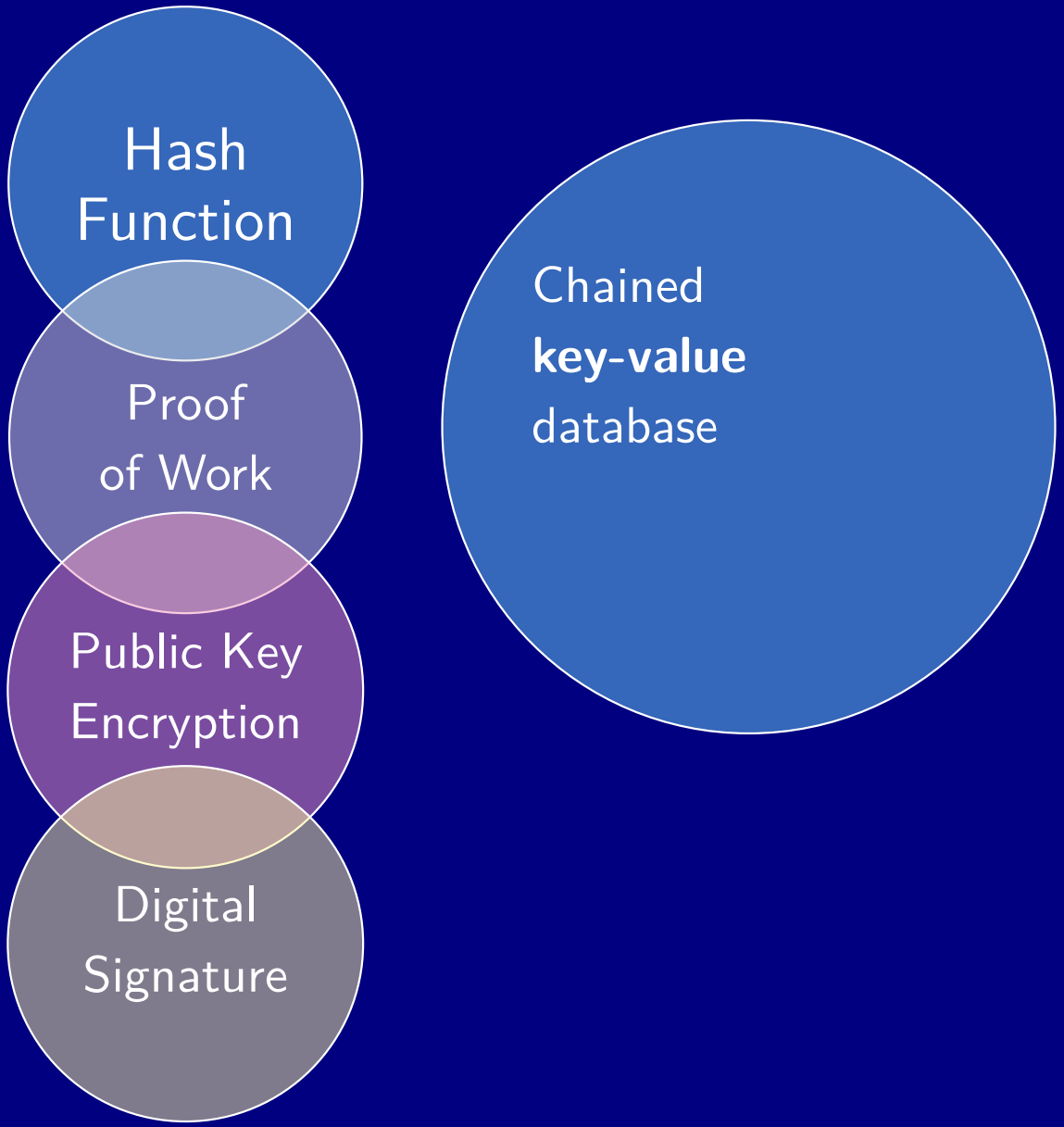
Characteristics

- No authority
- High availability
- Replicated, robust
- Tamper evident
- Difficult to modify
- Conflicts resolved

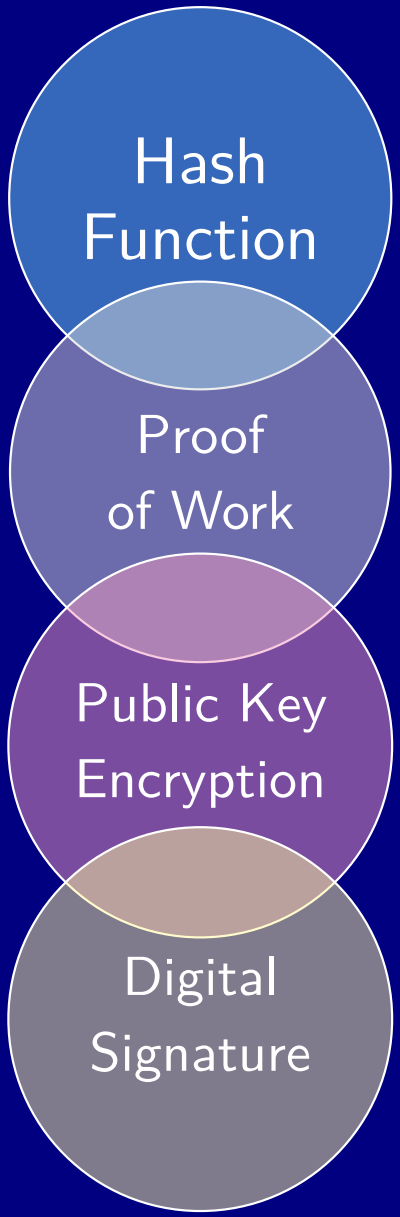
Dissect: Magical Ingredients & Recipe

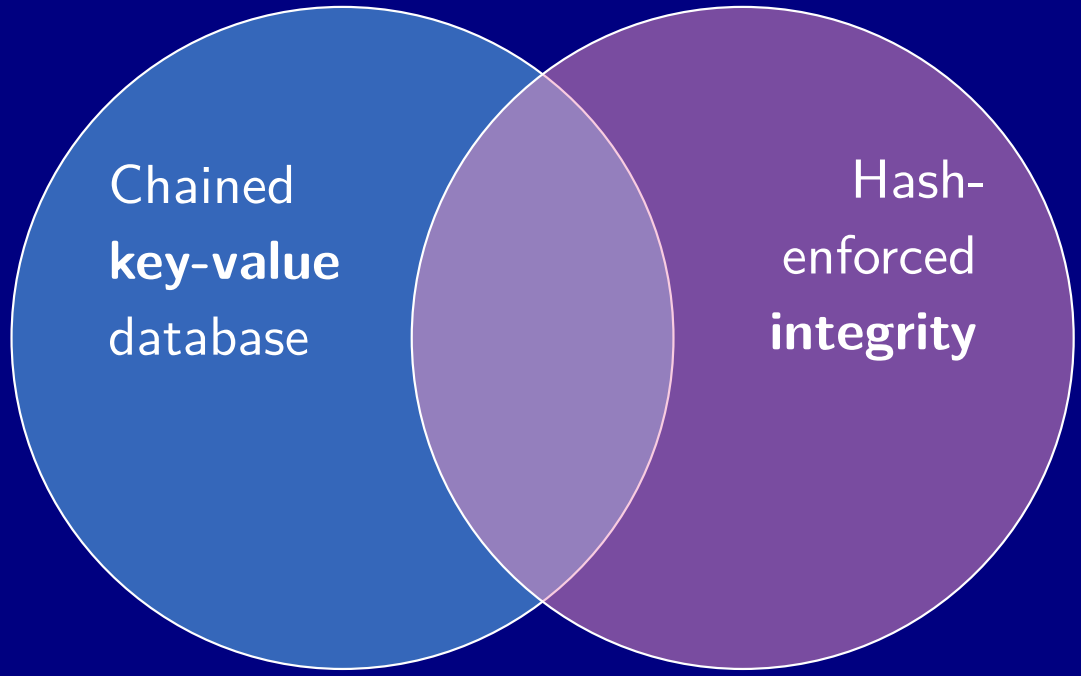


Dissect: Magical Ingredients & Recipe

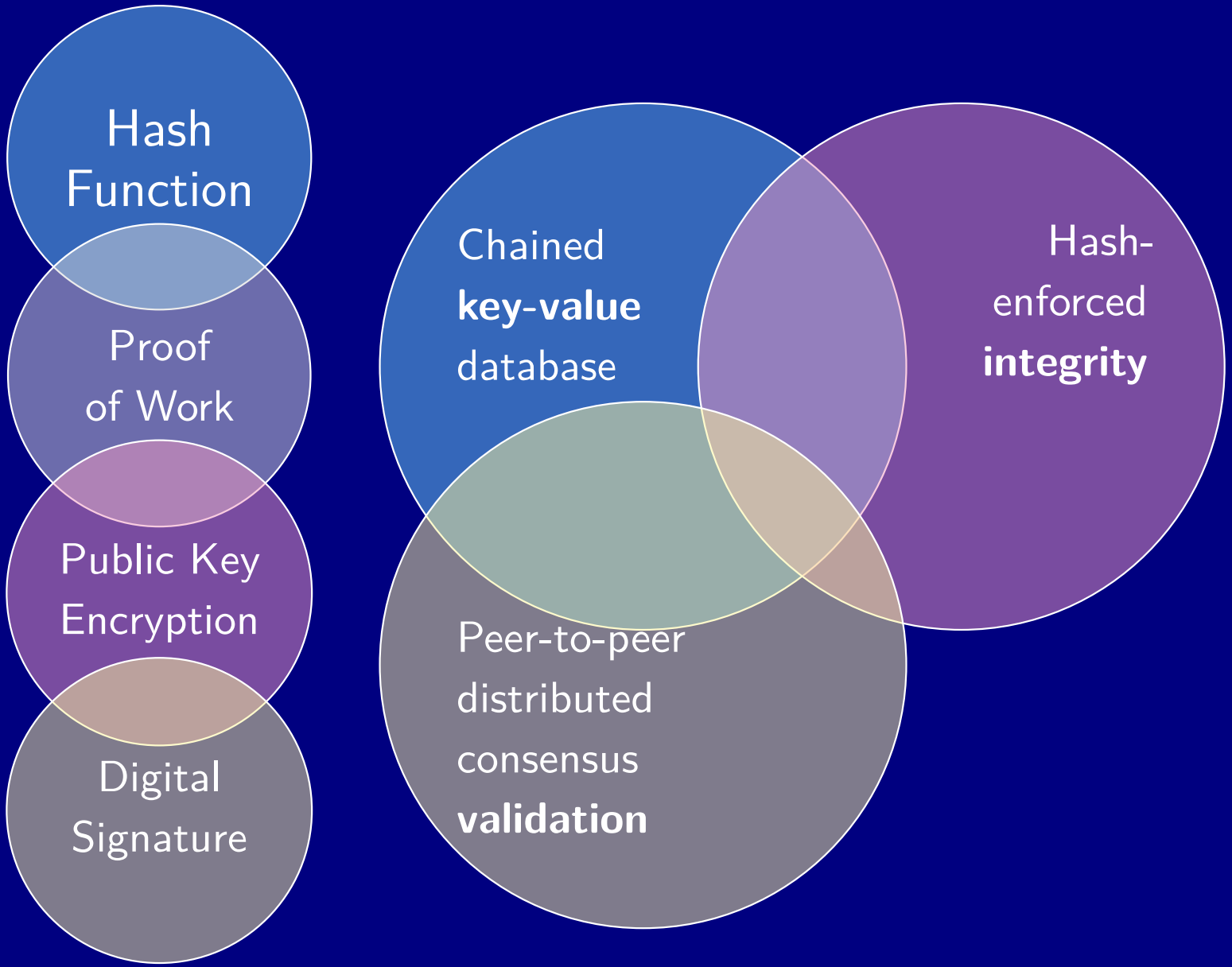


Dissect: Magical Ingredients & Recipe

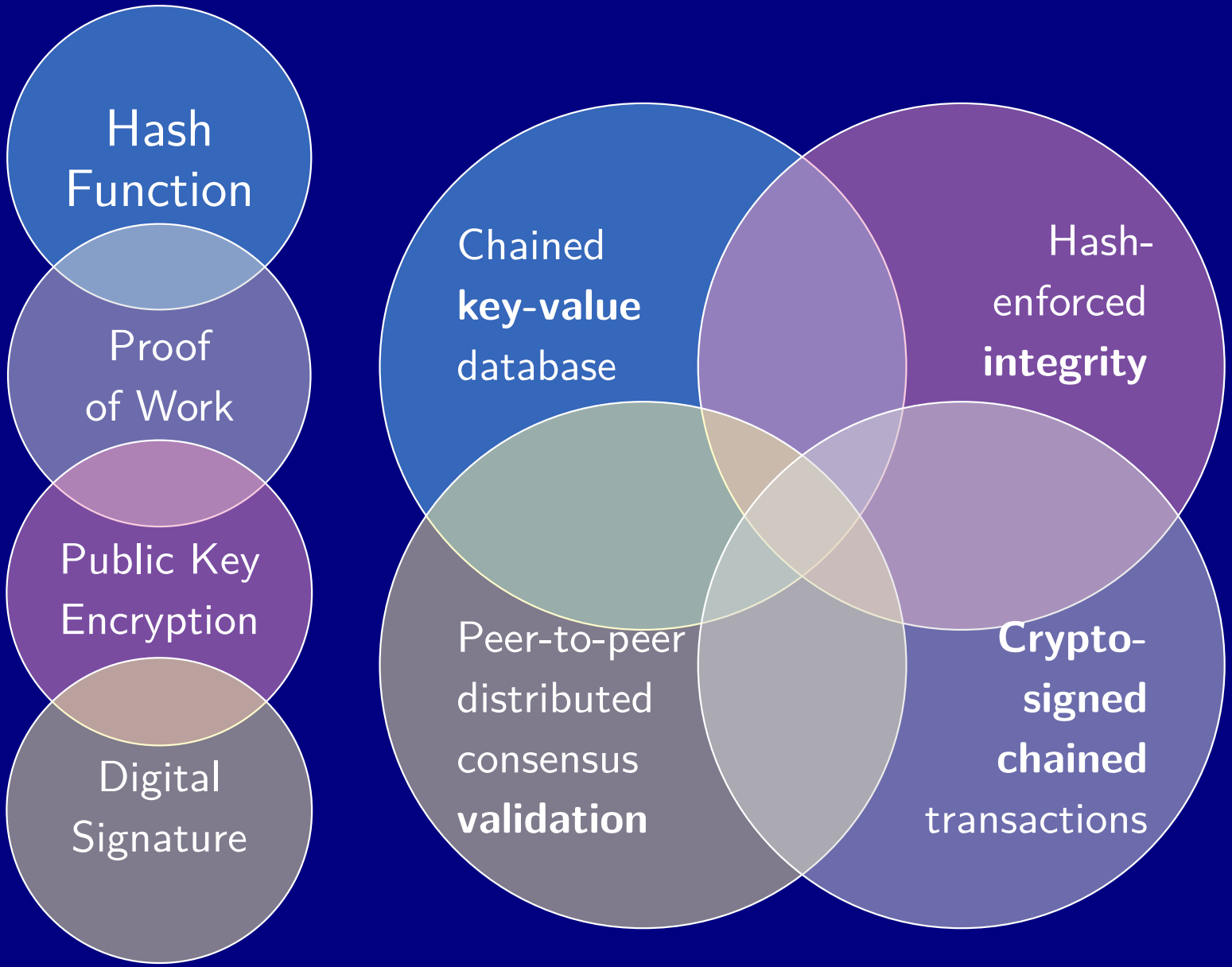




Dissect: Magical Ingredients & Recipe

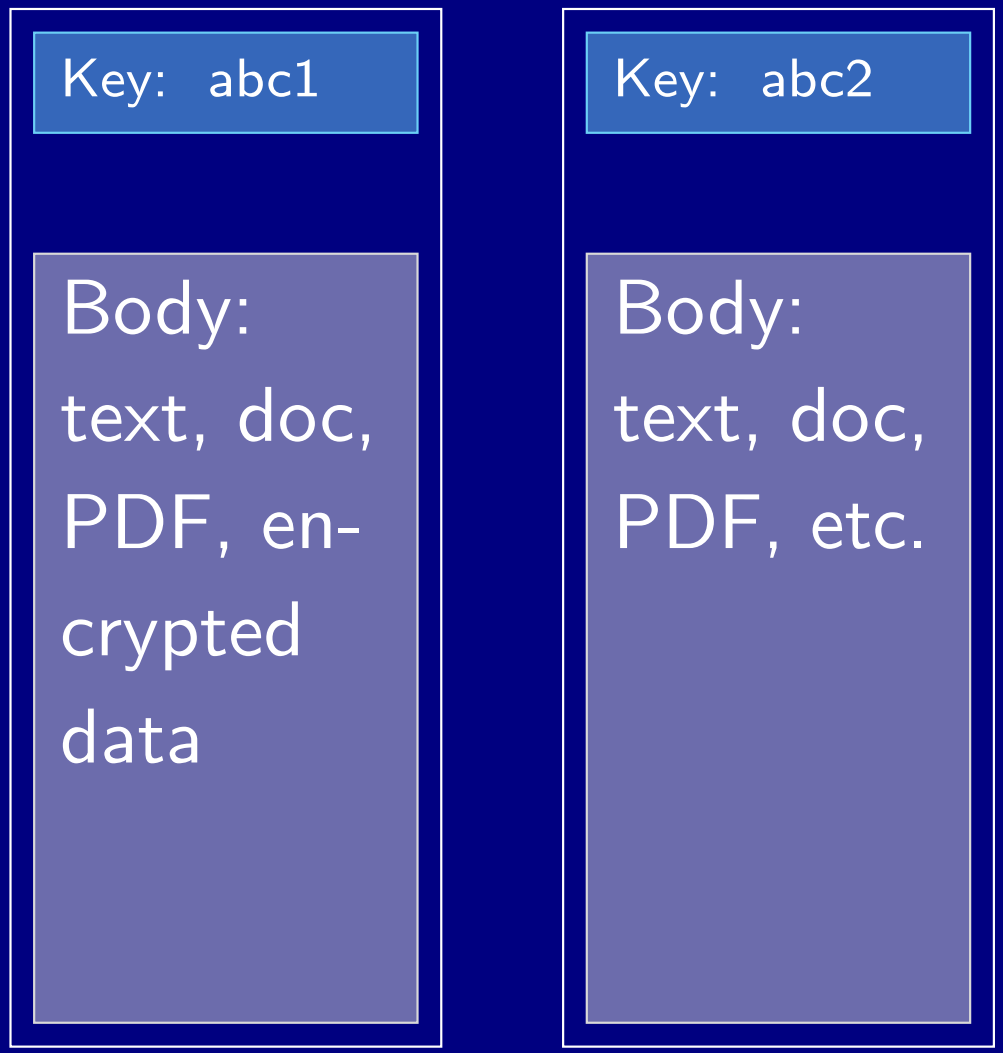


Dissect: Magical Ingredients & Recipe

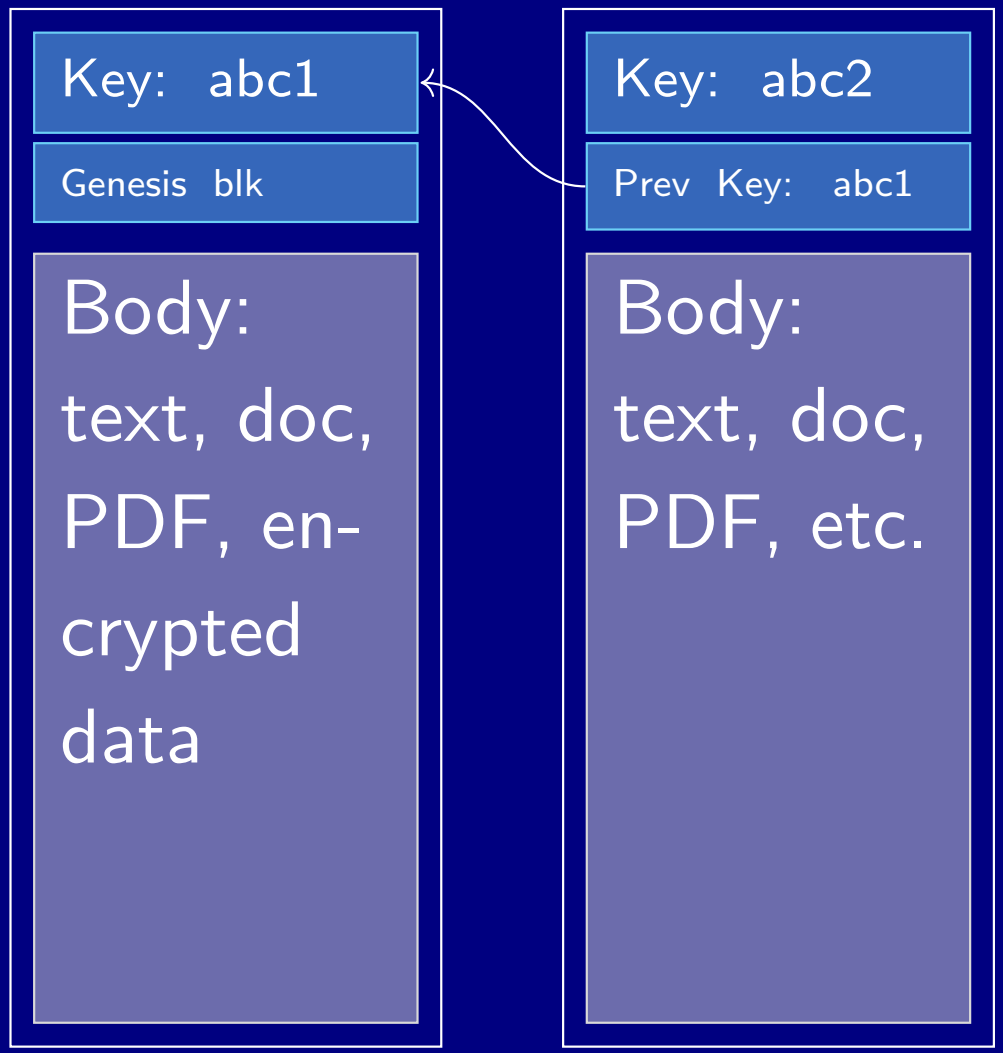


Ingredient 1: Chained Key-Value (Distributed) Database

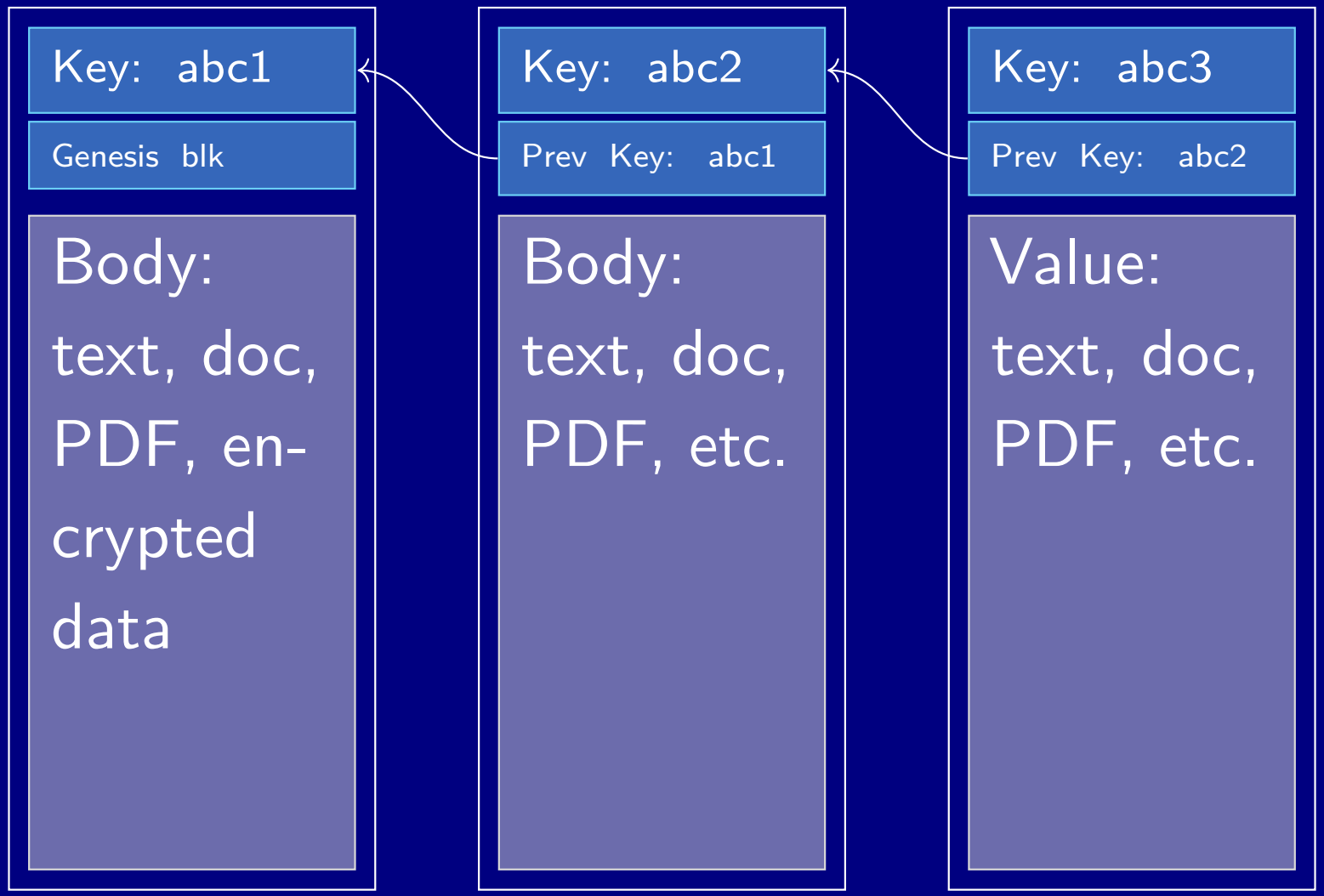
Ingredient 1: Chained Key-Value (Distributed) Database



Ingredient 1: Chained Key-Value (Distributed) Database



Ingredient 1: Chained Key-Value (Distributed) Database



Ingredient: Hash Functions

A **hash** H maps data of arbitrary size to a fixed size such that

- $H(x)$ is an easy to compute, deterministic function
- If $x \neq y$ then $H(x) \neq H(y)$ with high probability
- $H(x)$ appears random over its range as x varies
- IT hash function: first five letters of last name + first letter first name
- J. Smith problem
- Phone, zip, social, ...

Ingredient: Hash Functions

A **hash** H maps data of arbitrary size to a fixed size such that

- $H(x)$ is an easy to compute, deterministic function
- If $x \neq y$ then $H(x) \neq H(y)$ with high probability
- $H(x)$ appears random over its range as x varies
- IT hash function: first five letters of last name + first letter first name
- J. Smith problem
- Phone, zip, social, ...

A **cryptographic** hash function

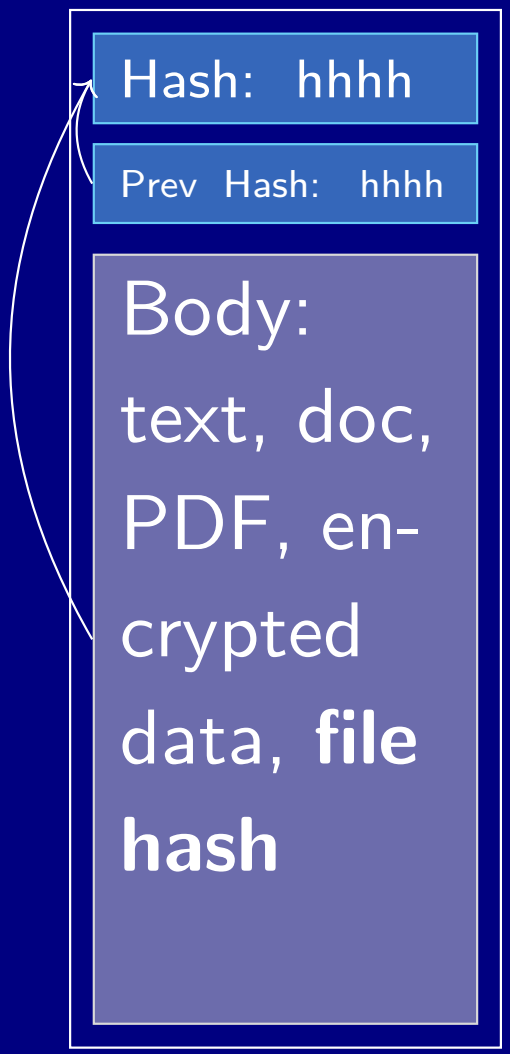
- Given y it is **very hard** to find x with $H(x) = y$
- **Fuggedaboutit** hard

SHA256 Cryptographic Hash Function

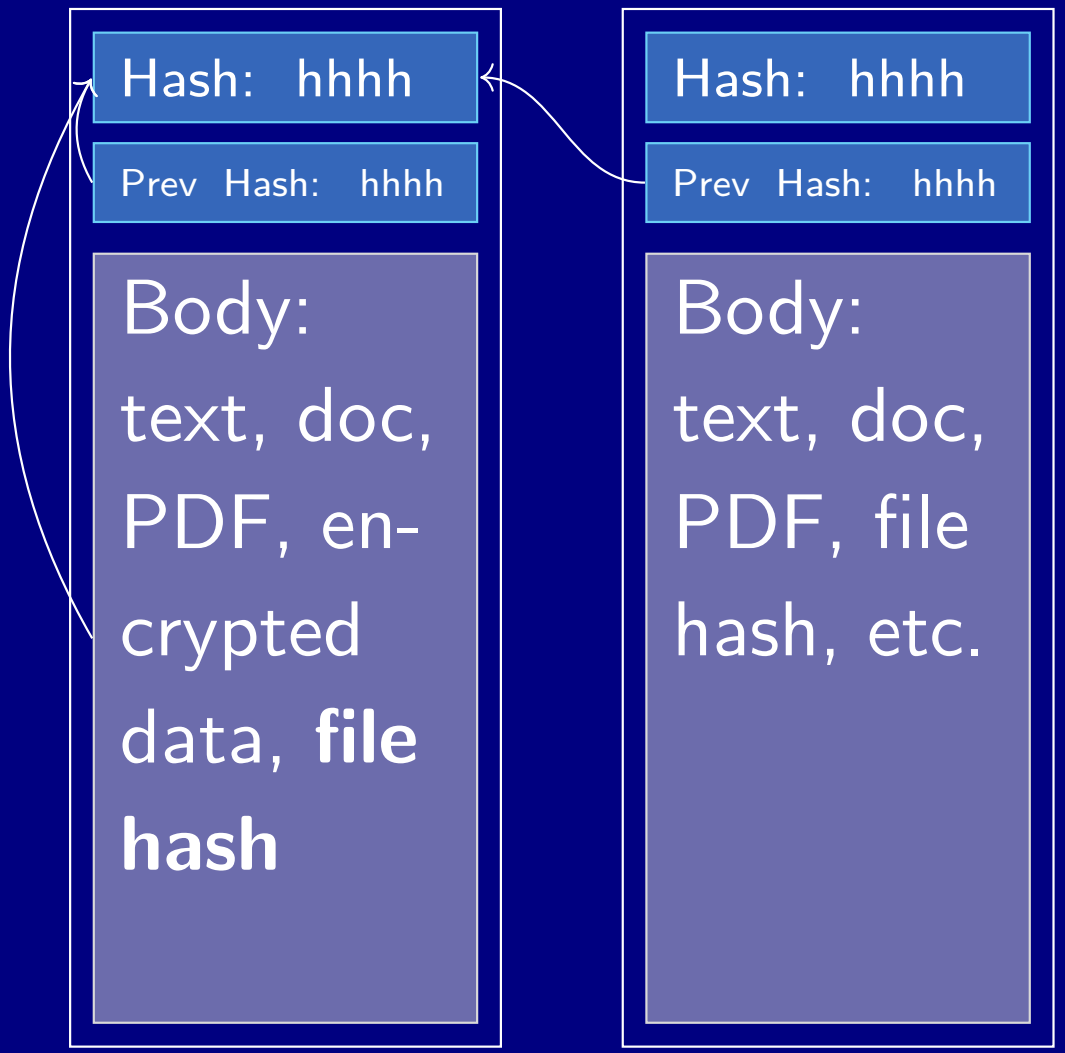
```
import hashlib

hashlib.sha256(b'The quick brown fox jumps over the lazy dog').hexdigest()
>>> 'd7a8fbb307d7809469ca9abcb0082e4f8d5651e46d3cdb762d02d0bf37c9e592'

hashlib.sha256(b'The quick brown fox jumps over the lazy dog.').hexdigest()
>>> 'ef537f25c895bfa782526529a9b63d97aa631564d5d789c2b765448c8635fb6c'
```

- Output = **very** large integer, between 0 and $2^{256} \approx 10^{77}$
- Specify input and output formats **very carefully**
- Probability of J. Smith collision: won't happen in lifetime of our universe

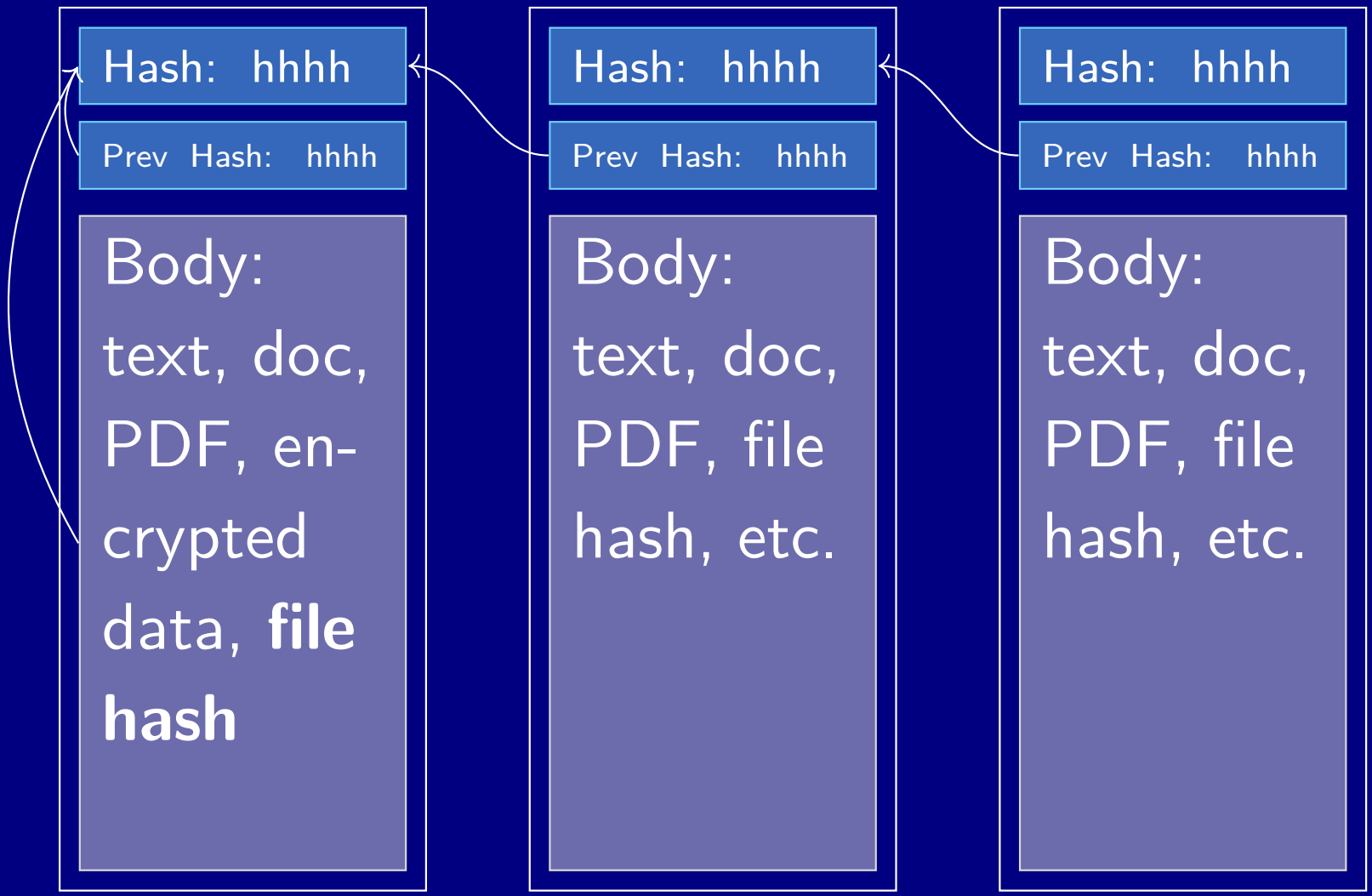
Ingredient 2: Hash-Enforced **Integrity**



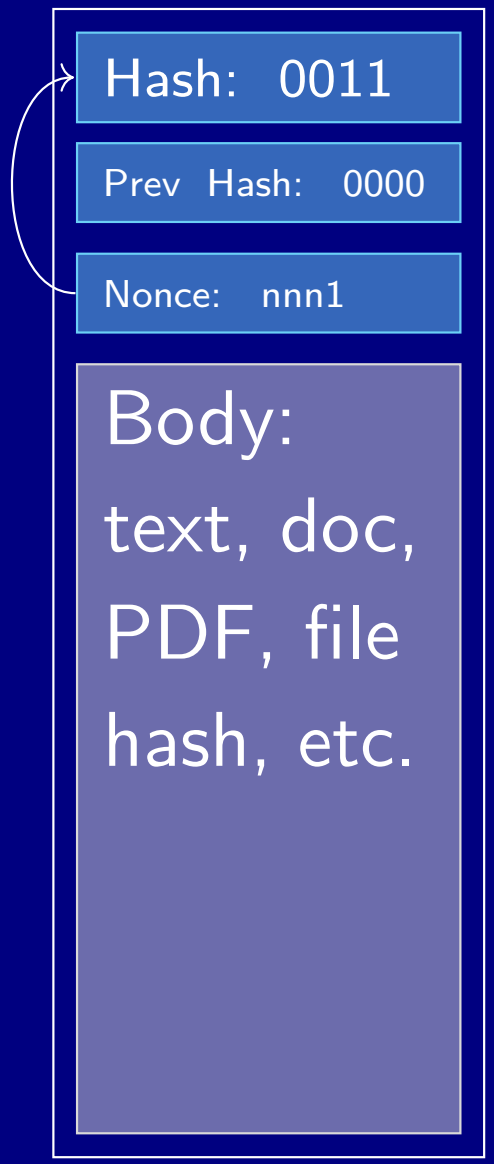
Ingredient 2: Hash-Enforced **Integrity**



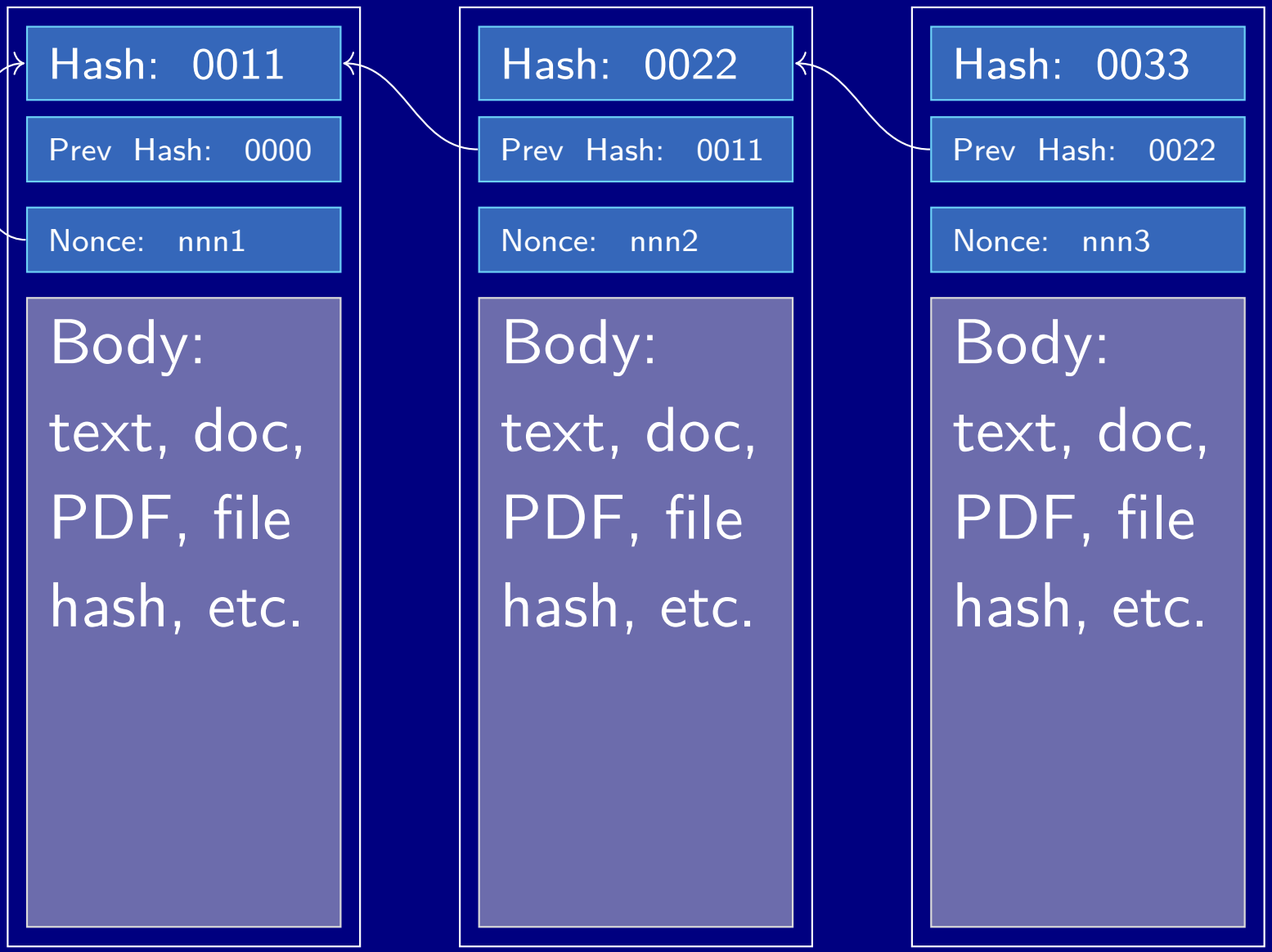
Ingredient 2: Hash-Enforced **Integrity**



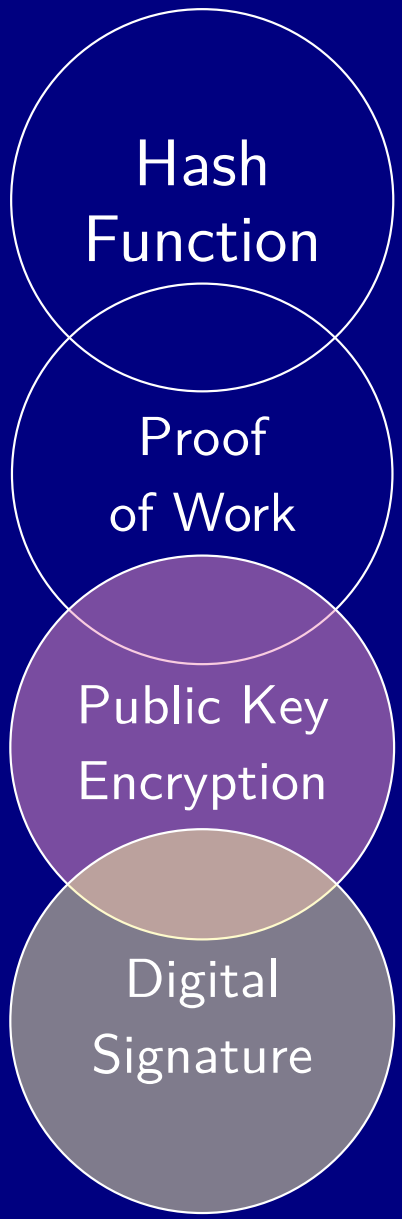
Ingredient 3: Distributed Validation and **Proof-Of-Work**

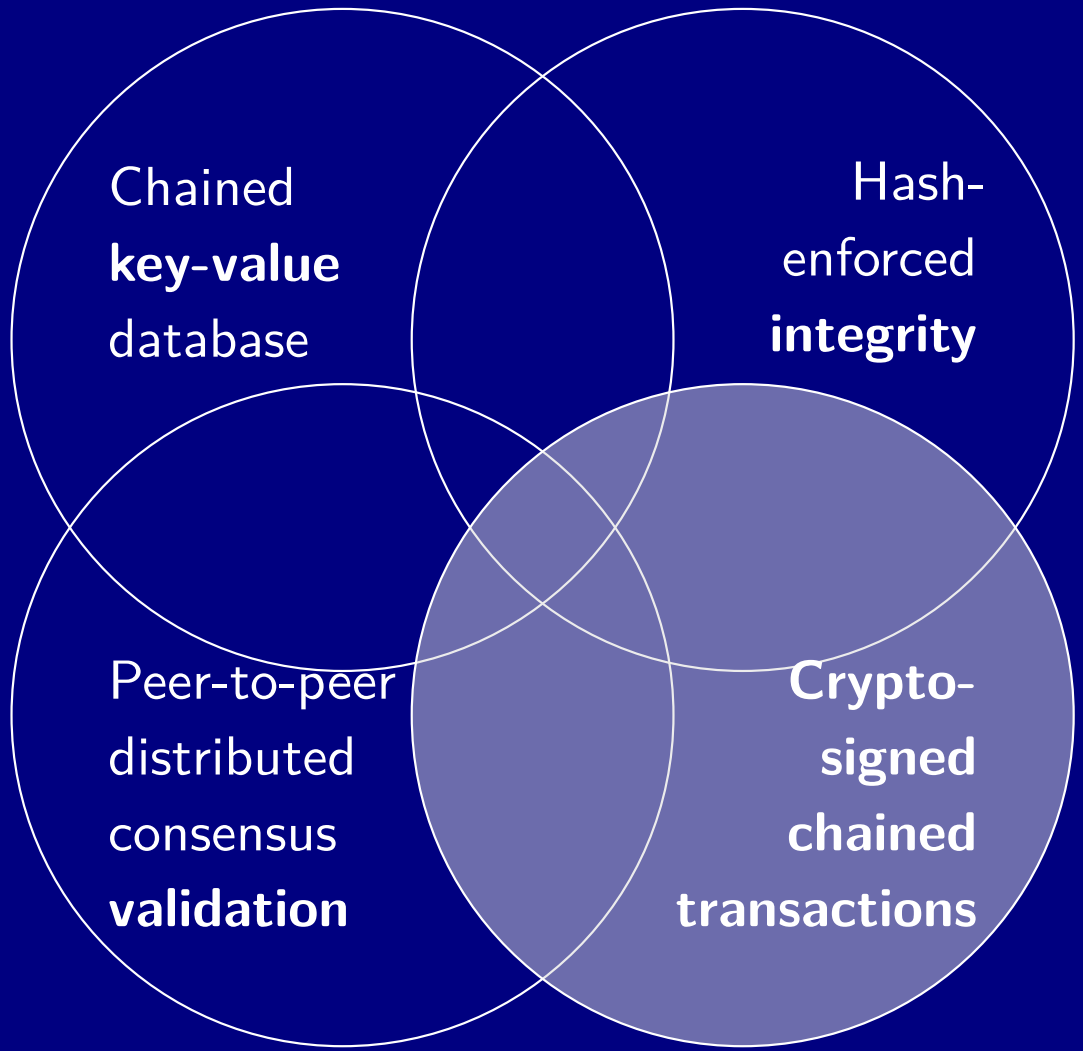


Ingredient 3: Distributed Validation and **Proof-Of-Work**

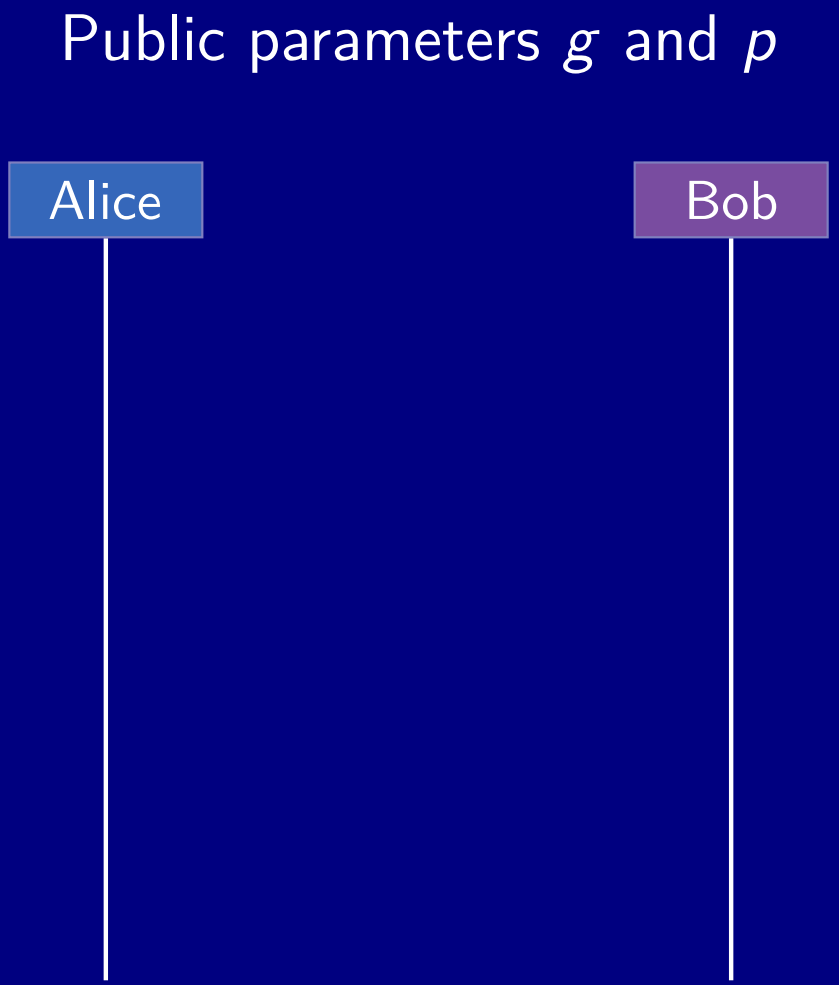


Dissect: Cryptographic Ingredients

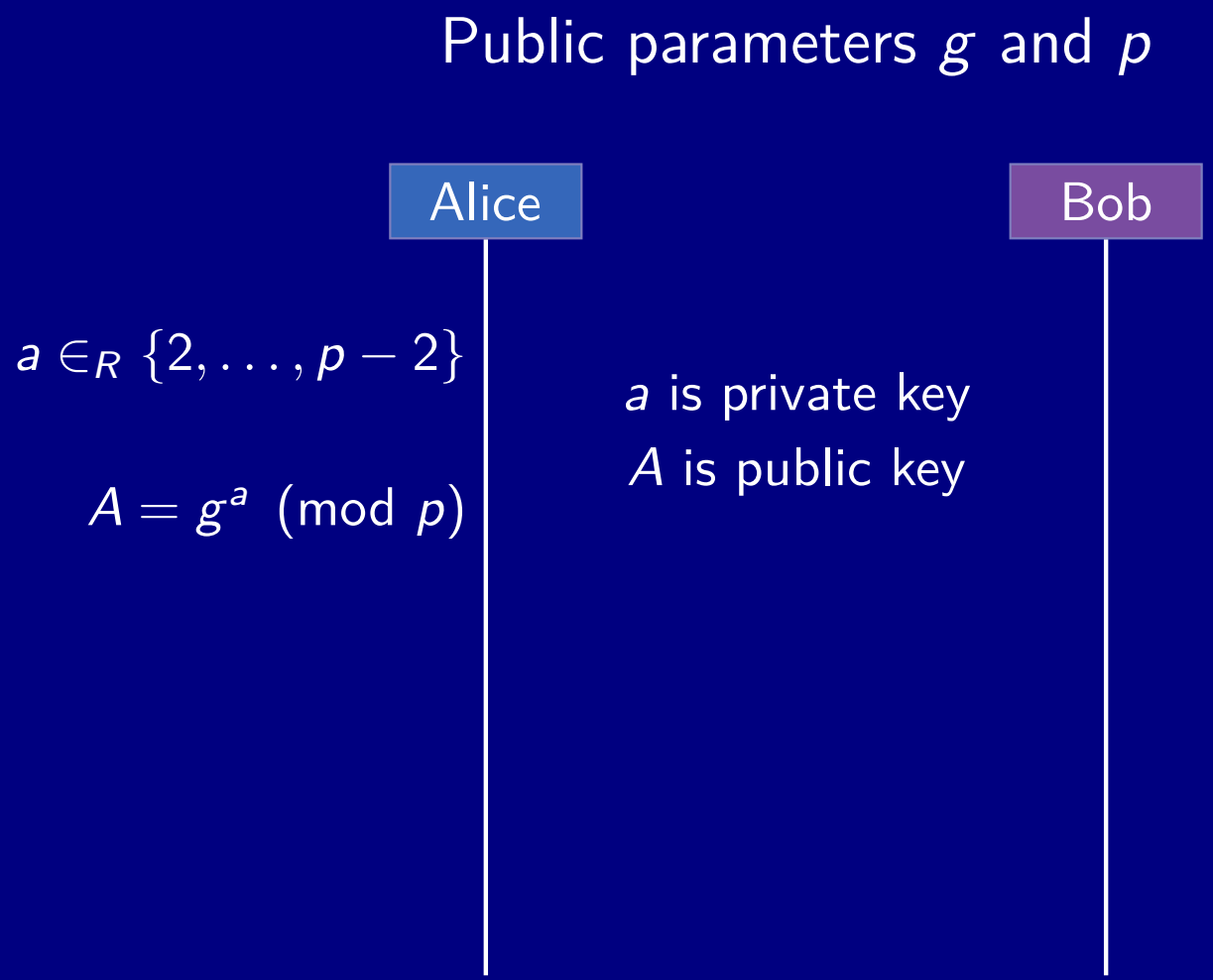




Creating a Shared Secret



Creating a Shared Secret



Public/private pair (A, a) are cryptographically linked but a is hidden

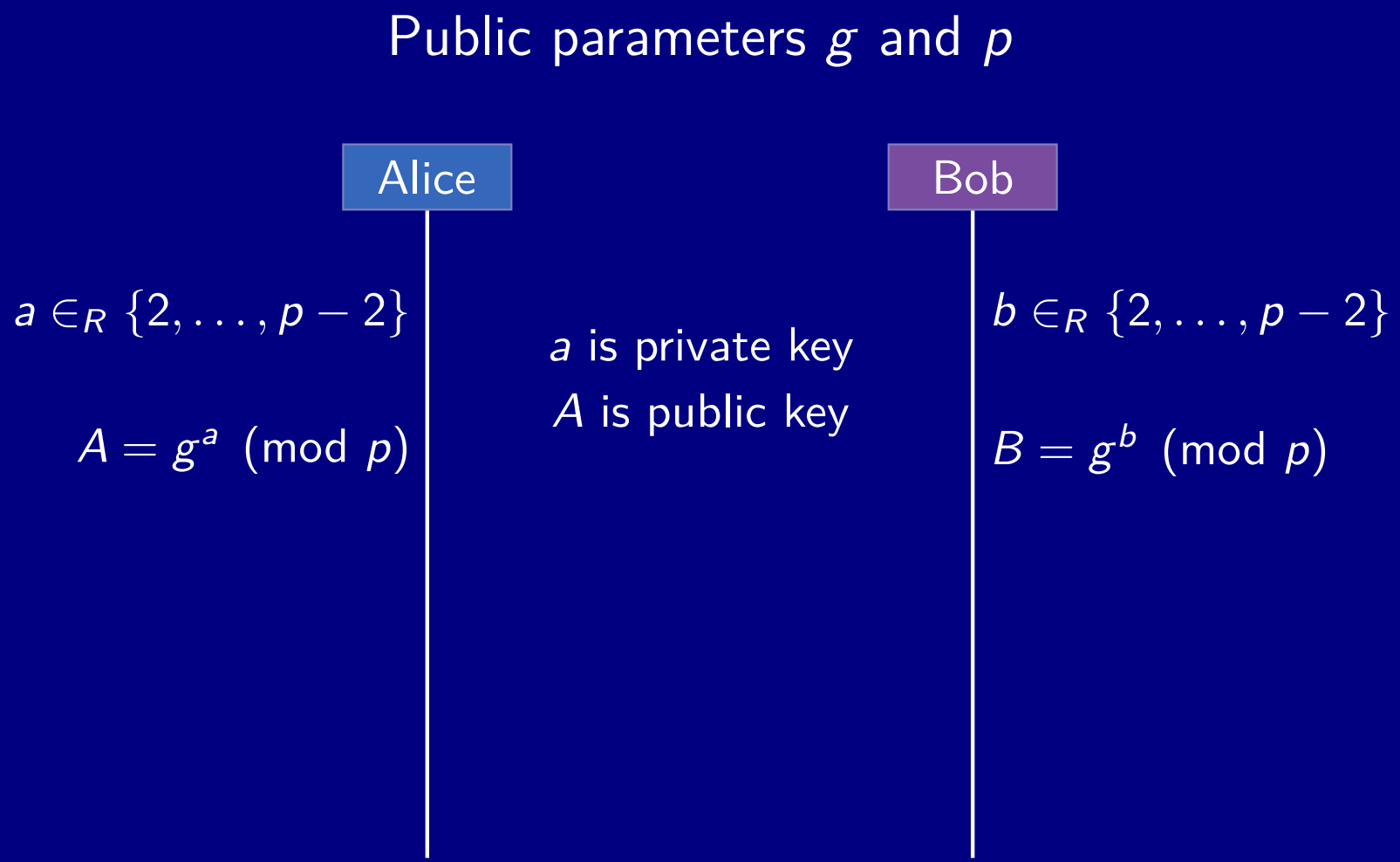
Why is Public/Private Key Pair $(A = g^a, a)$ Secure?

Graph of $a \mapsto g^a \pmod{p}$

- mod p means remainder when dividing by p
- Not smooth like log/exp
- Graph essentially random
- Given a can compute g^a quickly...
- ...but can't go backwards...
- Given g^a can only find a by brute force

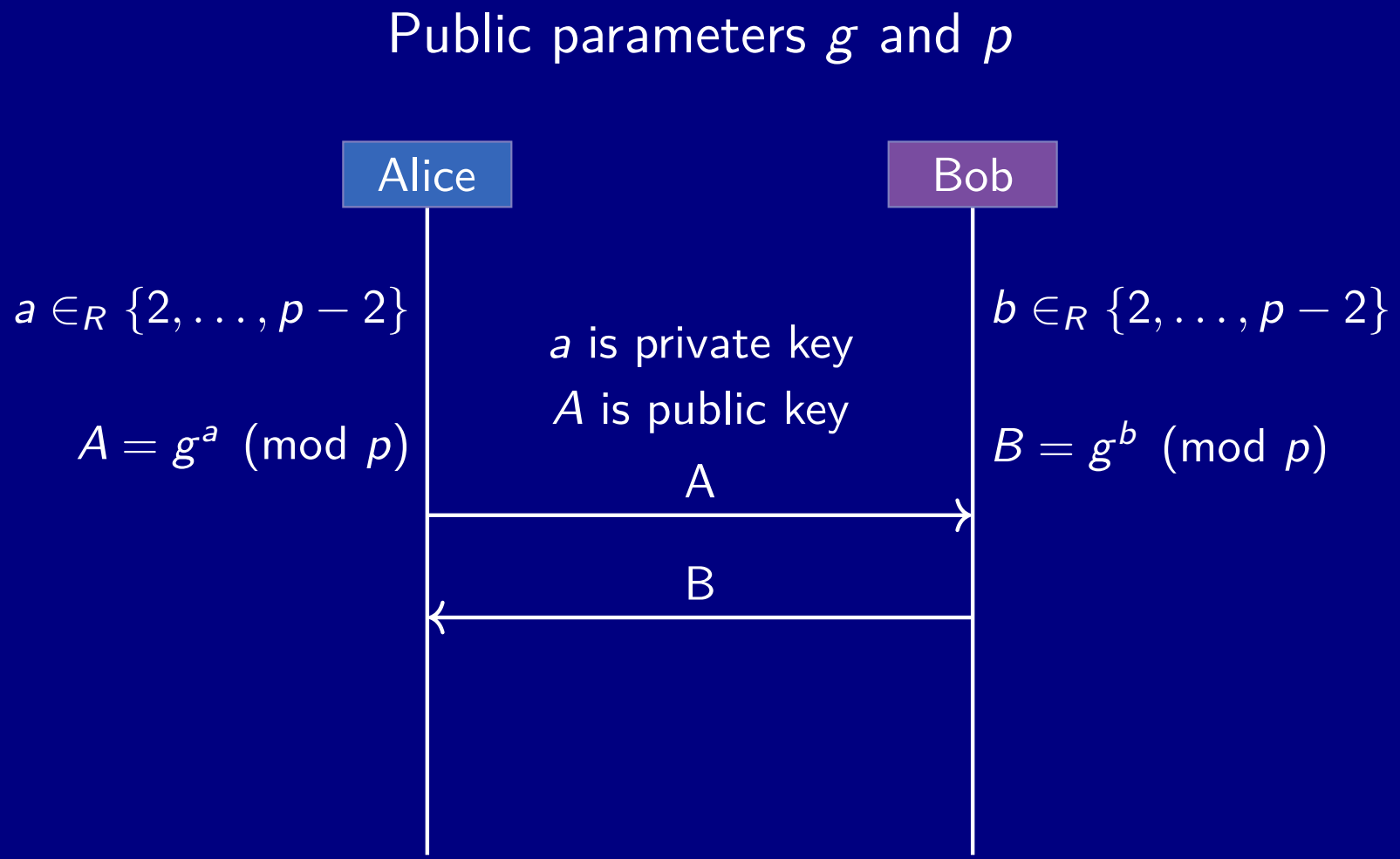
Graph shows powers of $g = 3$ modulo $p = 100043$; $100042 = 2 \times 50021$ is twice a prime.

Creating a Shared Secret



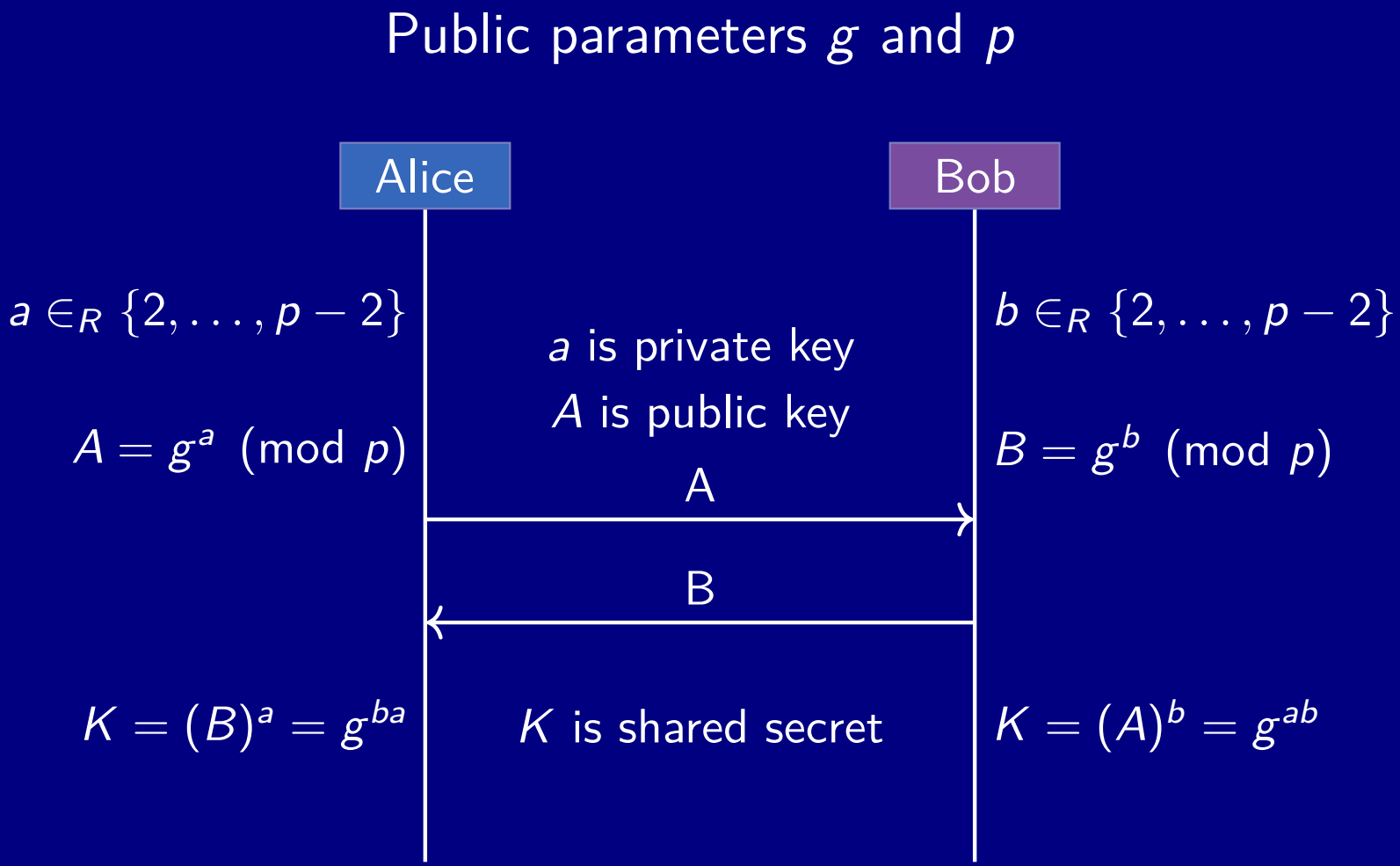
Public/private pair (A, a) are cryptographically linked but a is hidden

Creating a Shared Secret



Public/private pair (A, a) are cryptographically linked but a is hidden

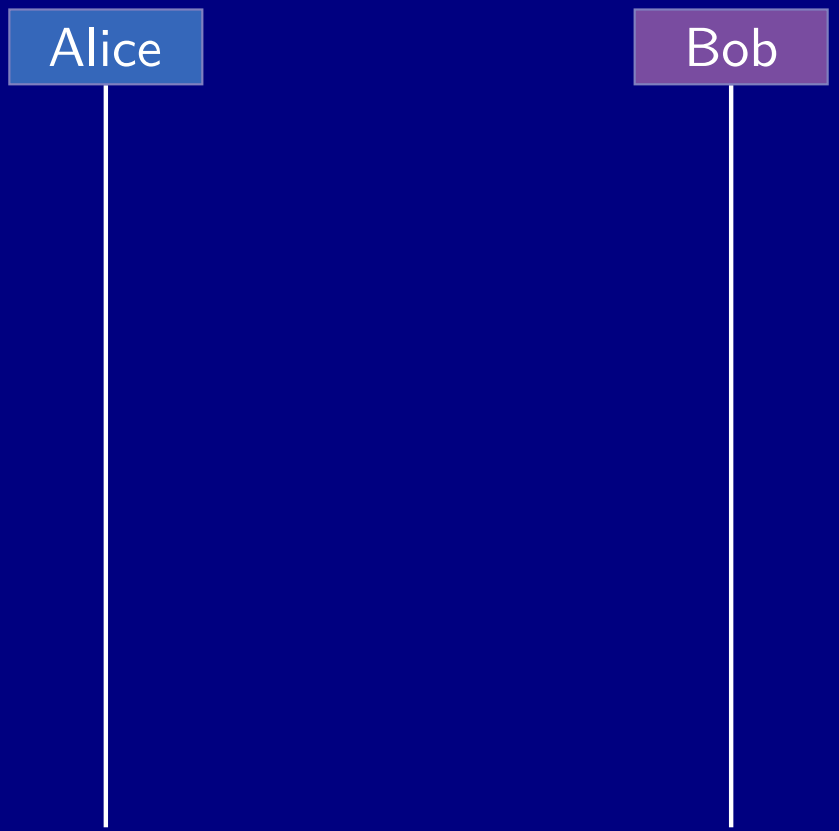
Creating a Shared Secret



Public/private pair (A, a) are cryptographically linked but a is hidden

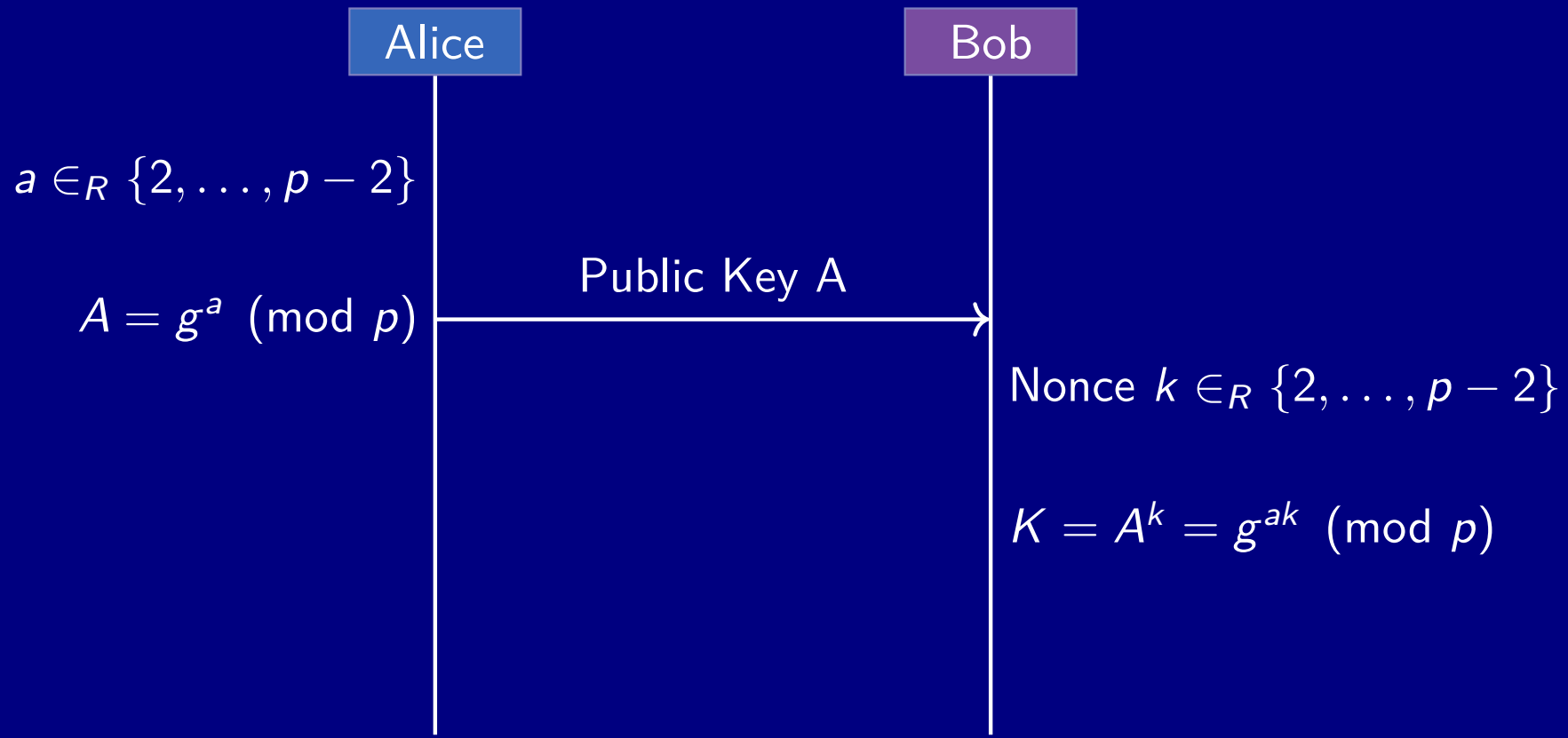
ElGamel Public Key Encryption

Public parameters g and p
Send message m from Bob to Alice



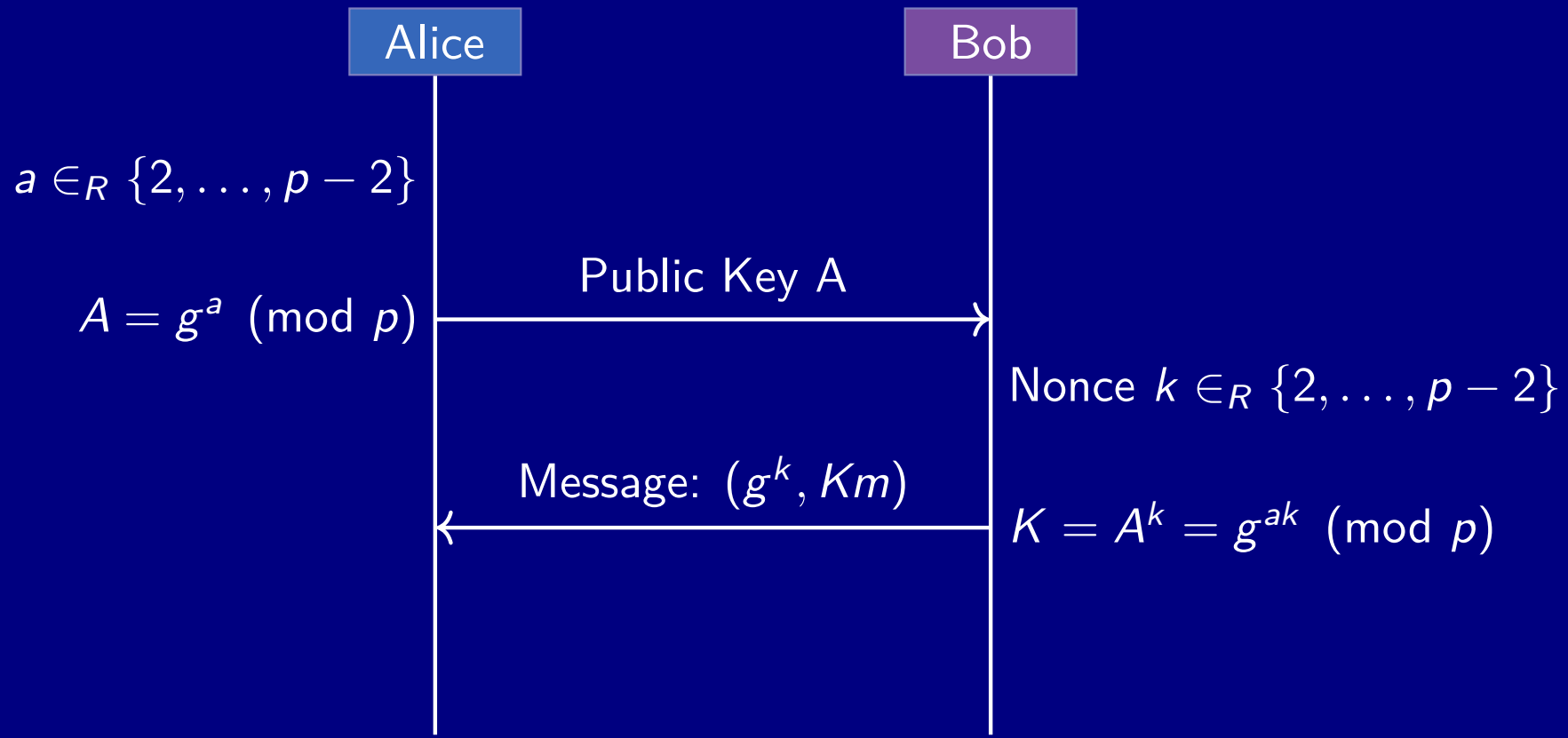
ElGamel Public Key Encryption

Public parameters g and p
Send message m from Bob to Alice



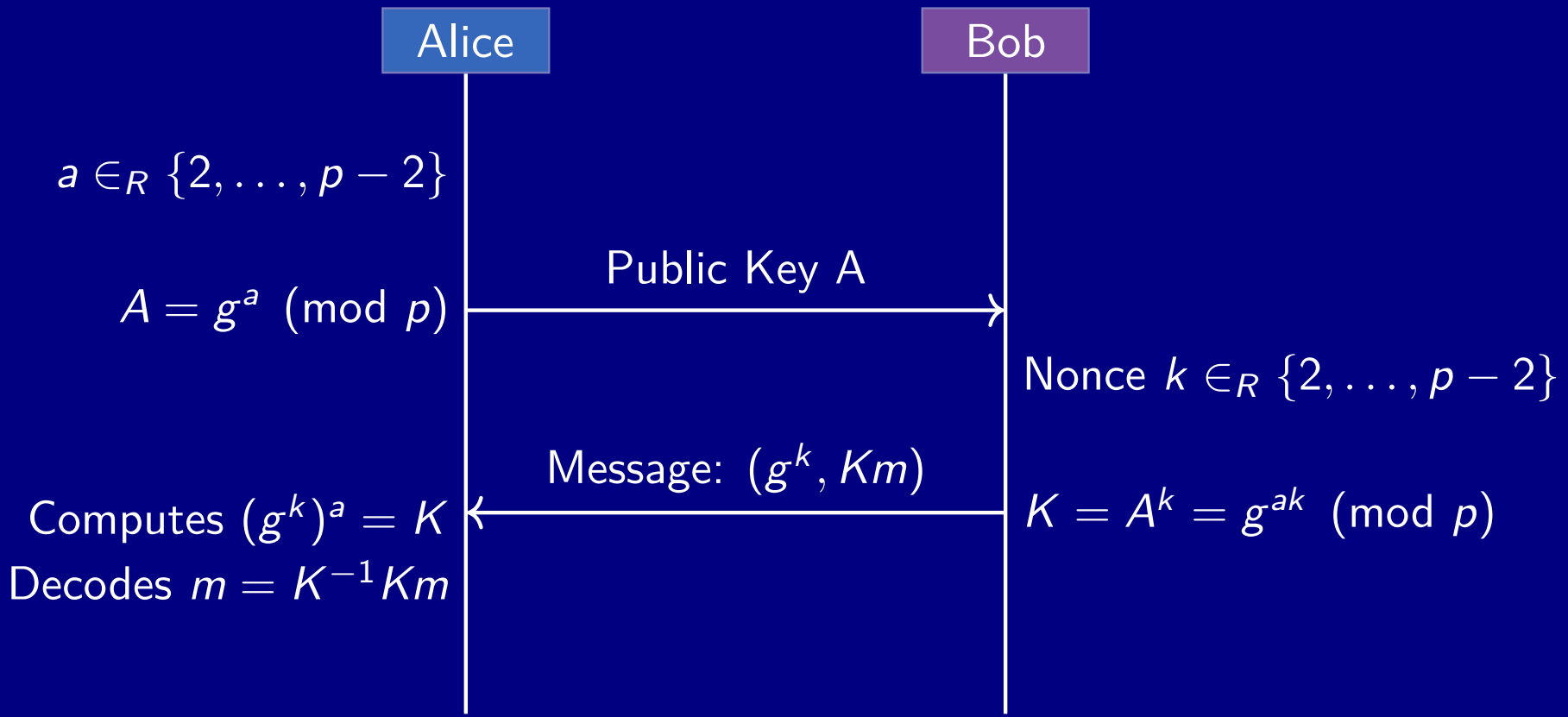
ElGamel Public Key Encryption

Public parameters g and p
Send message m from Bob to Alice



ElGamel Public Key Encryption

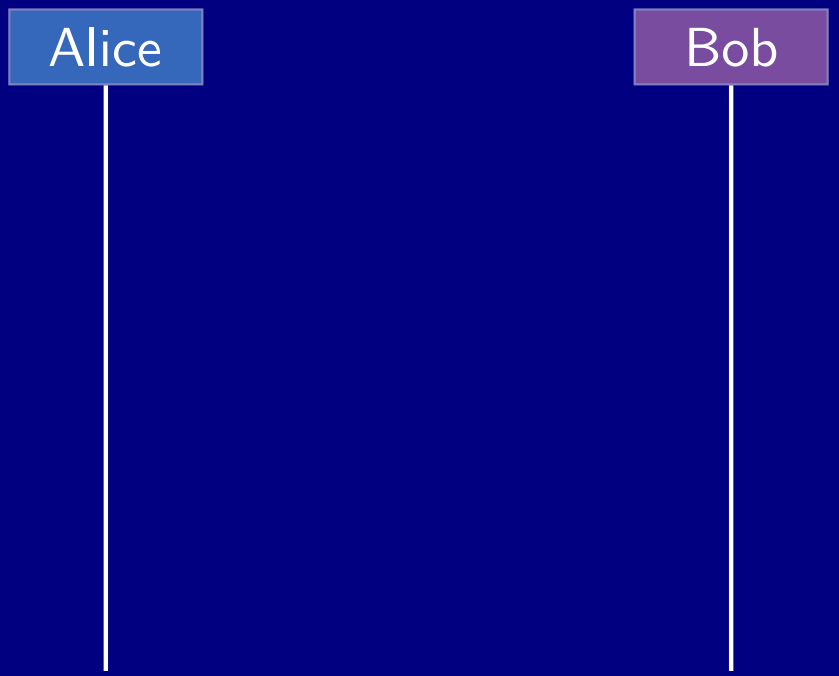
Public parameters g and p
Send message m from Bob to Alice



g^k conveys information about k but shields its value; K hides message m

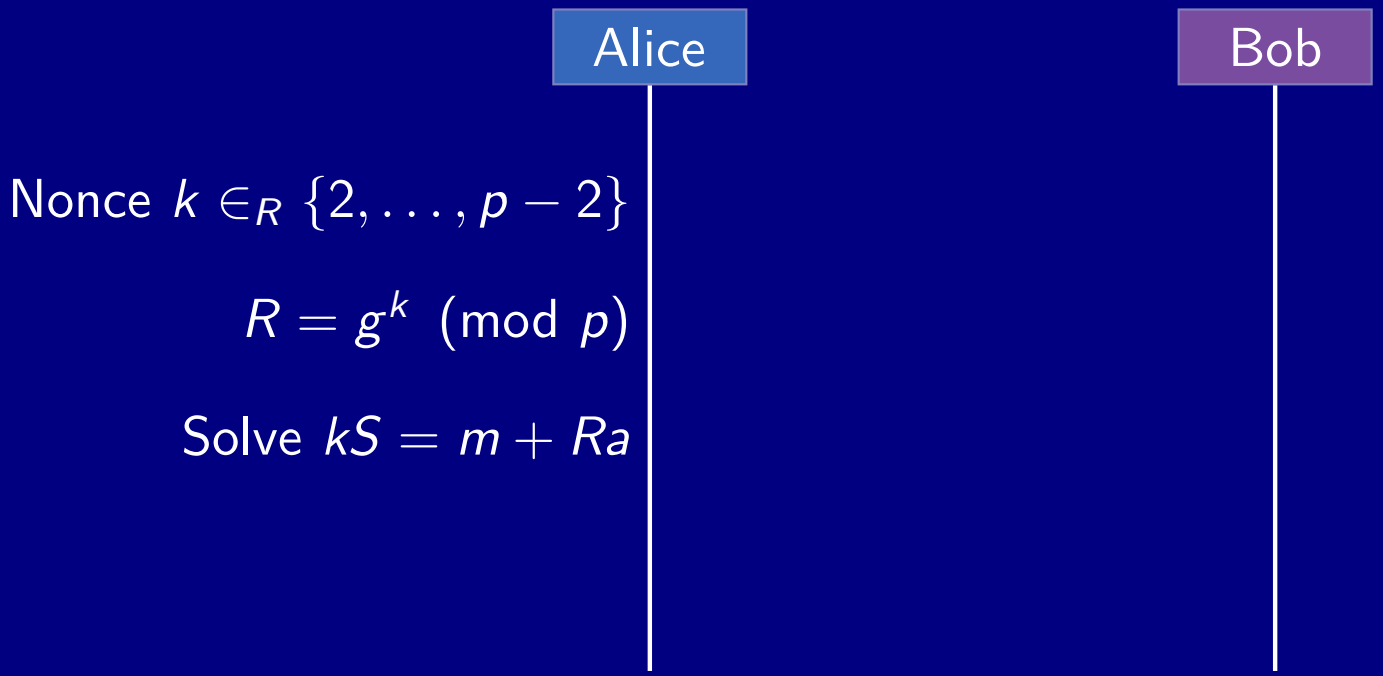
Digital Signature

Alice to sign message m, Bob to verify
$g, p, A = g^a, m$ all public, a is secret



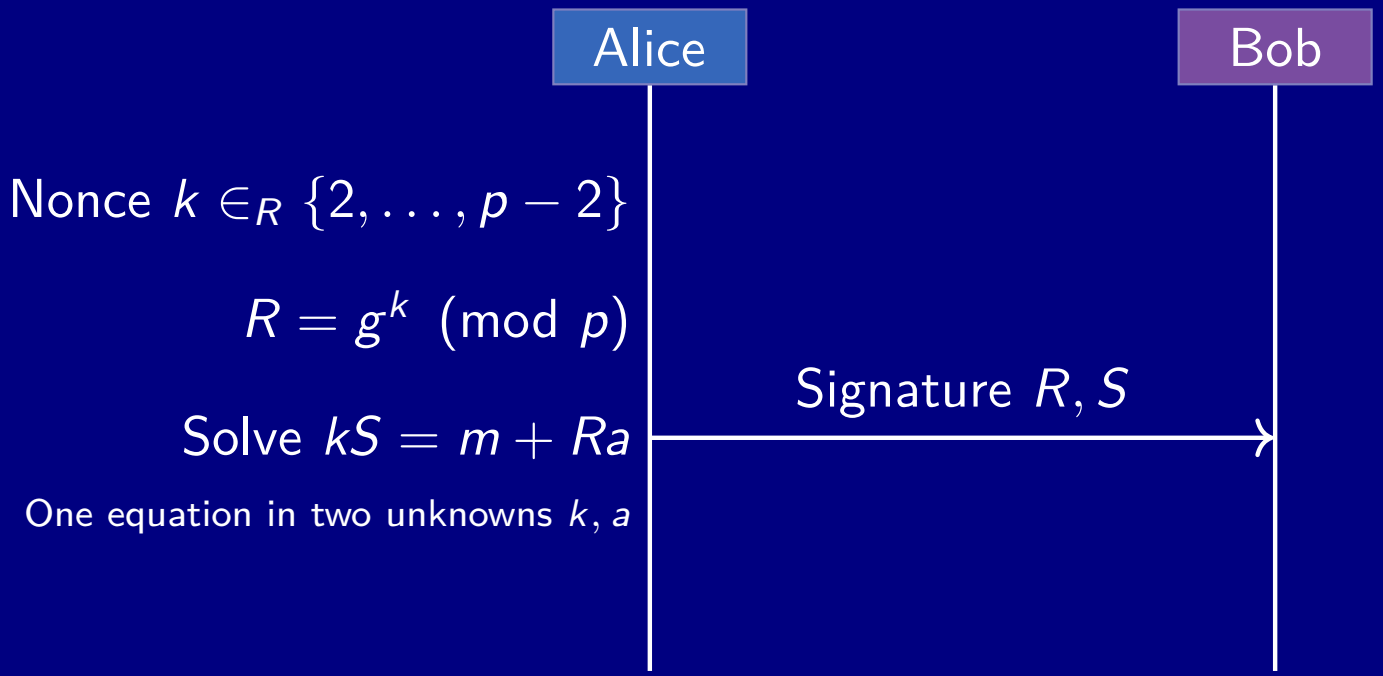
Digital Signature

Alice to sign message m, Bob to verify
$g, p, A = g^a, m$ all public, a is secret



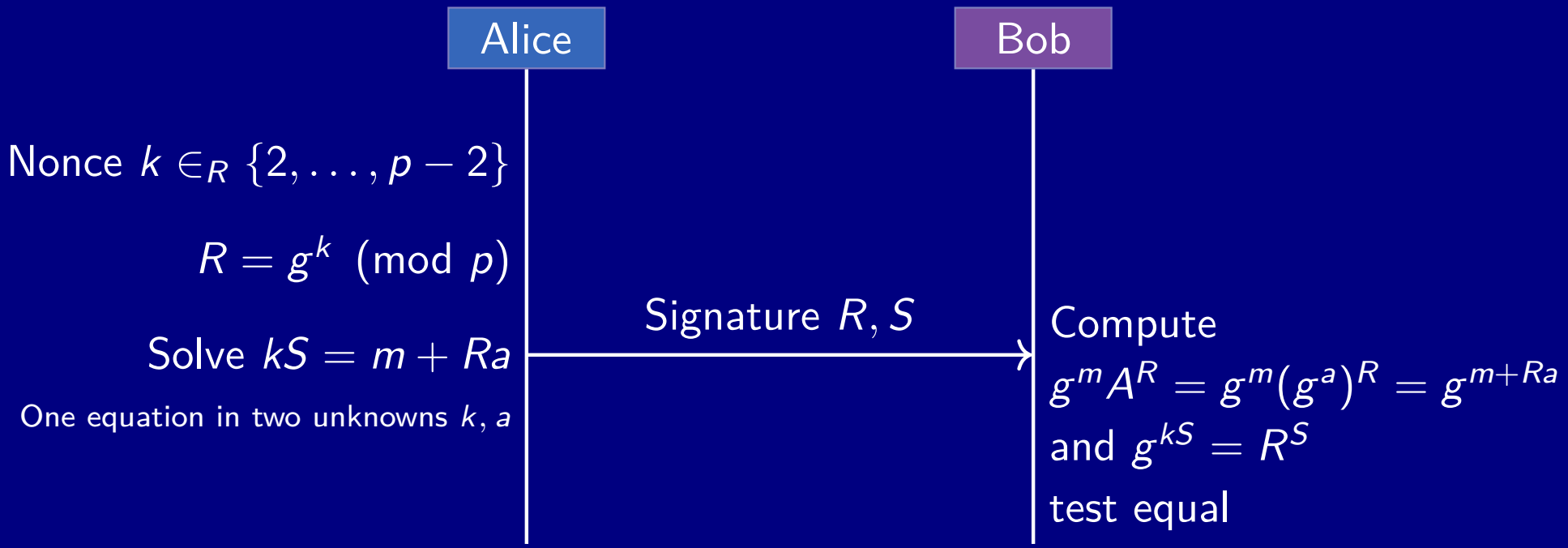
Digital Signature

Alice to sign message m, Bob to verify
$g, p, A = g^a, m$ all public, a is secret



Digital Signature

Alice to sign message m, Bob to verify
$g, p, A = g^a, m$ all public, a is secret



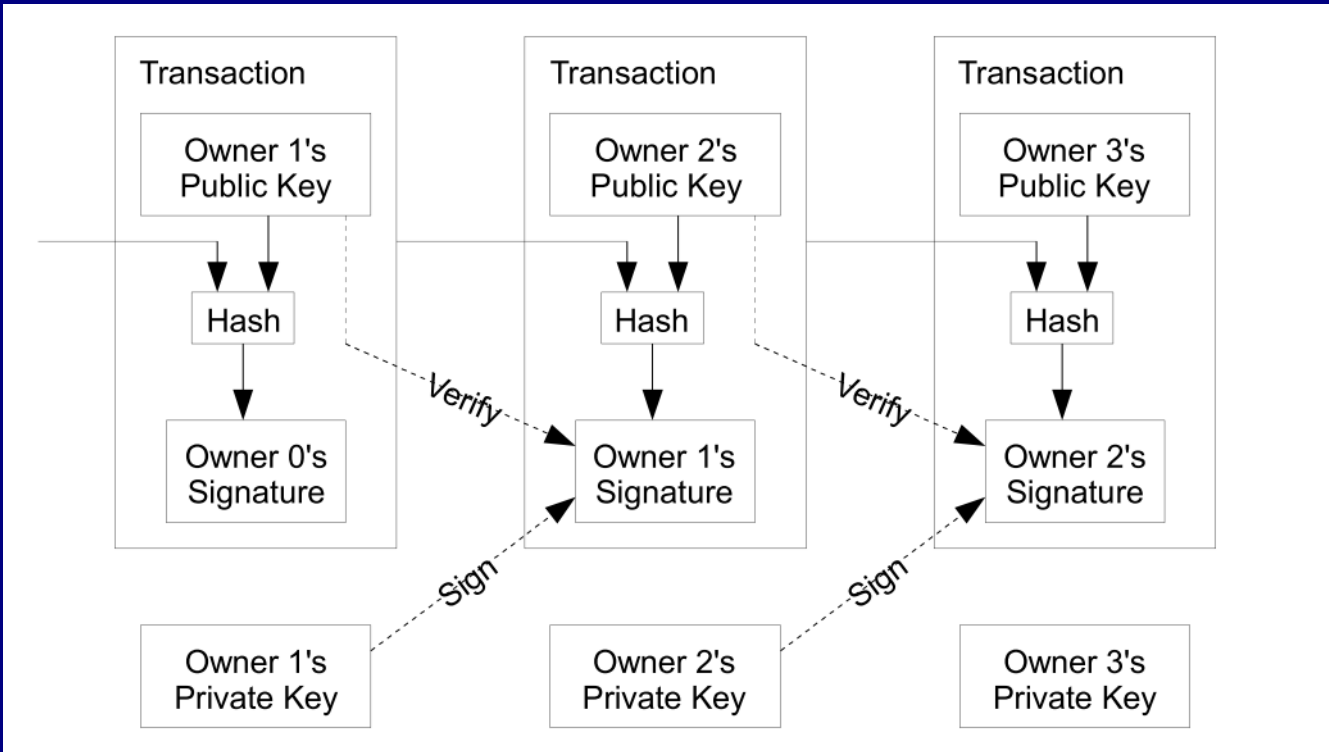
If Alice does not know a she can't find R, S to solve $R^S = g^m A^R$

Powerful Properties of Digital Signature

- Signer **authentication**: verifier assured that signature has been created only by sender who possess the corresponding secret private key
- Message **integrity**: if message modified, signature fails; signature tamper evident
- **Non-repudiation**: existence of signature proves it came from sender; sender cannot repudiate signing in future
- Wet ink signatures can be forged; document can be altered; signature can be denied

Ingredient 4: Double-spend mechanism

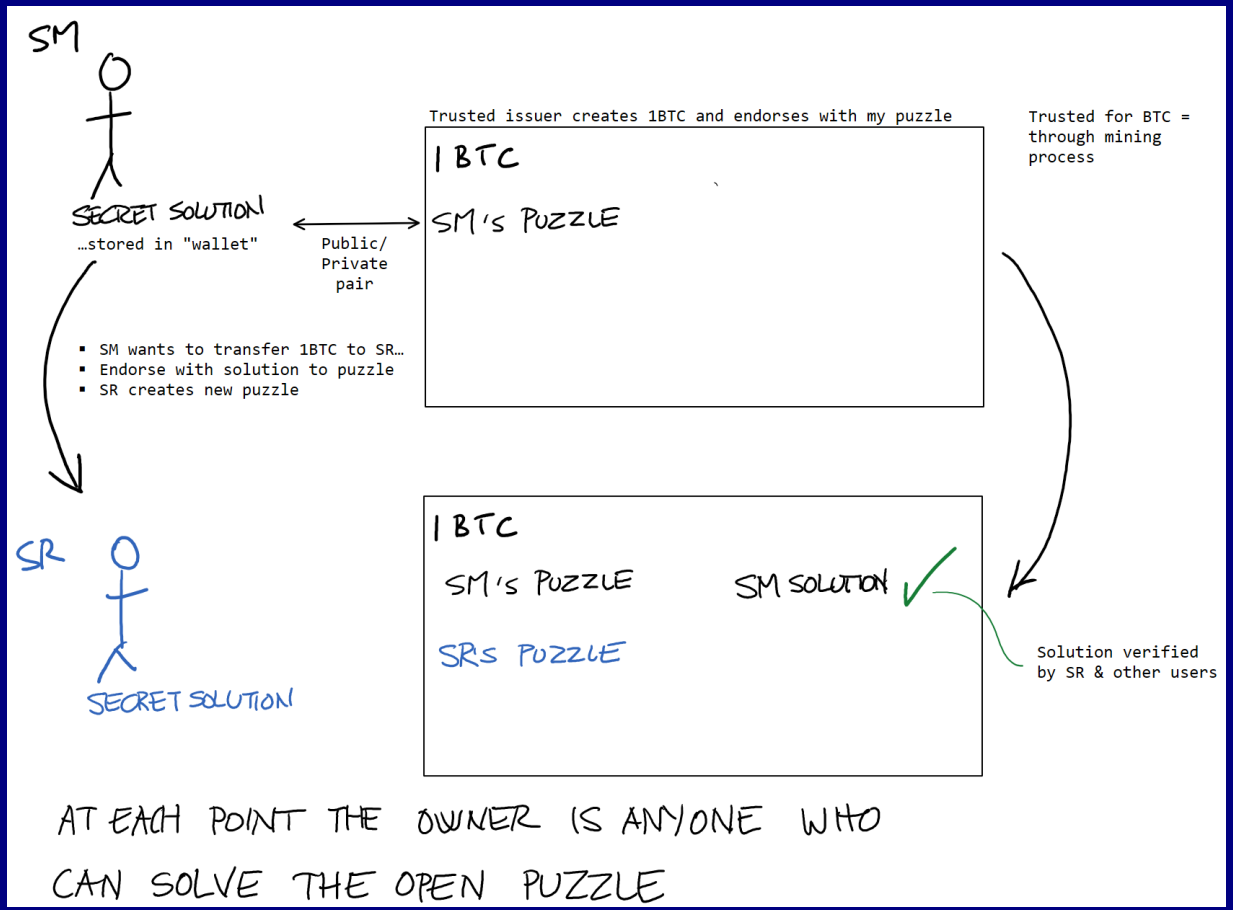
- Bitcoin ledger tracks coin ownership
- Owners can endorse to new owners in cryptographically secure manner
- Public pseudonymous chain of ownership



Bitcoin: A Peer to Peer Electronic Cash System, Satoshi Nakamoto (2008) https://bitcoin.org/bitcoin.pdf

Ingredient 4: Double-spend mechanism

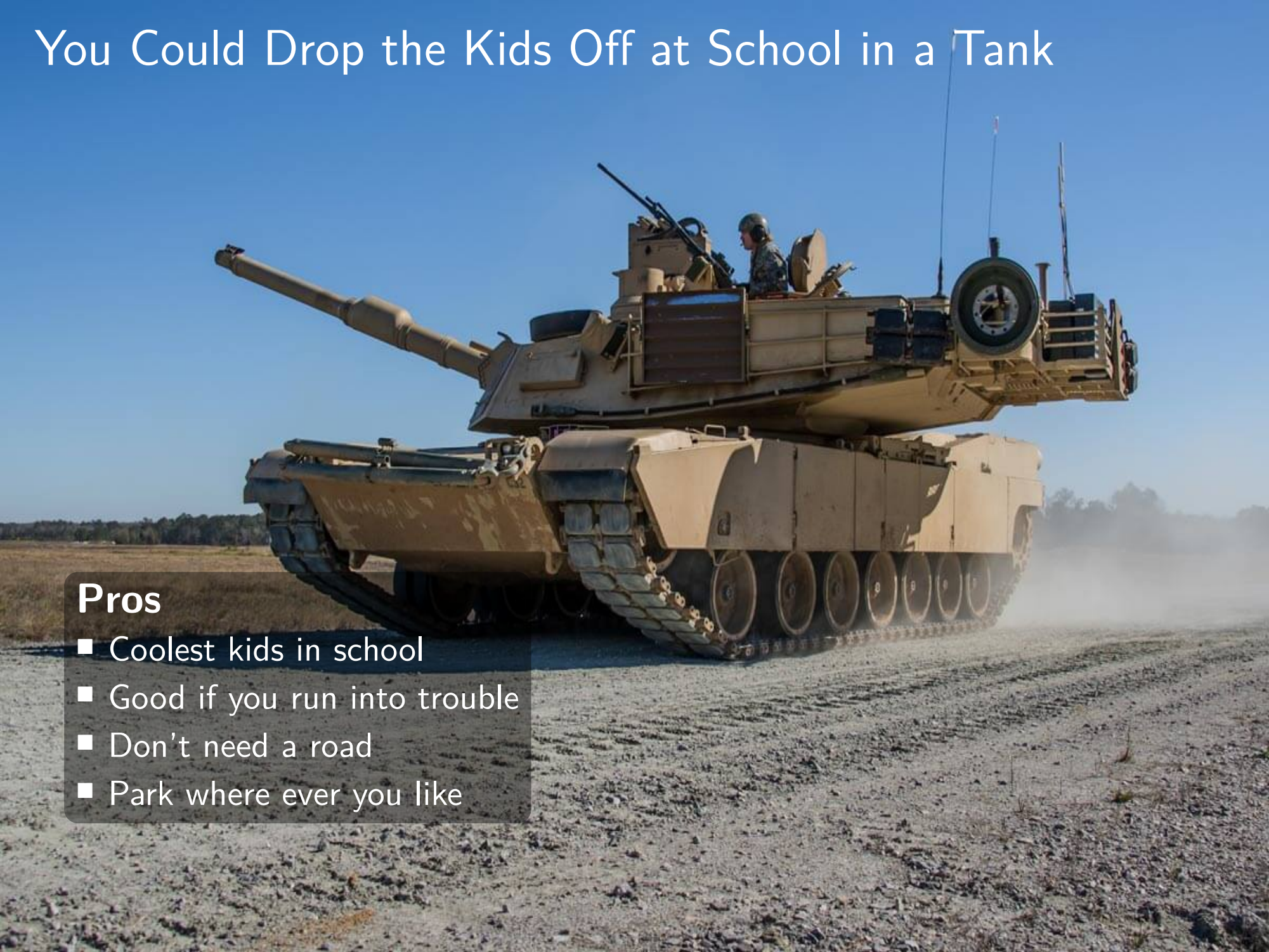
- Bitcoin ledger tracks coin ownership
- Owners can endorse to new owners in cryptographically secure manner
- Public pseudonymous chain of ownership



Where Are We?

You Could Drop the Kids Off at School in a Tank

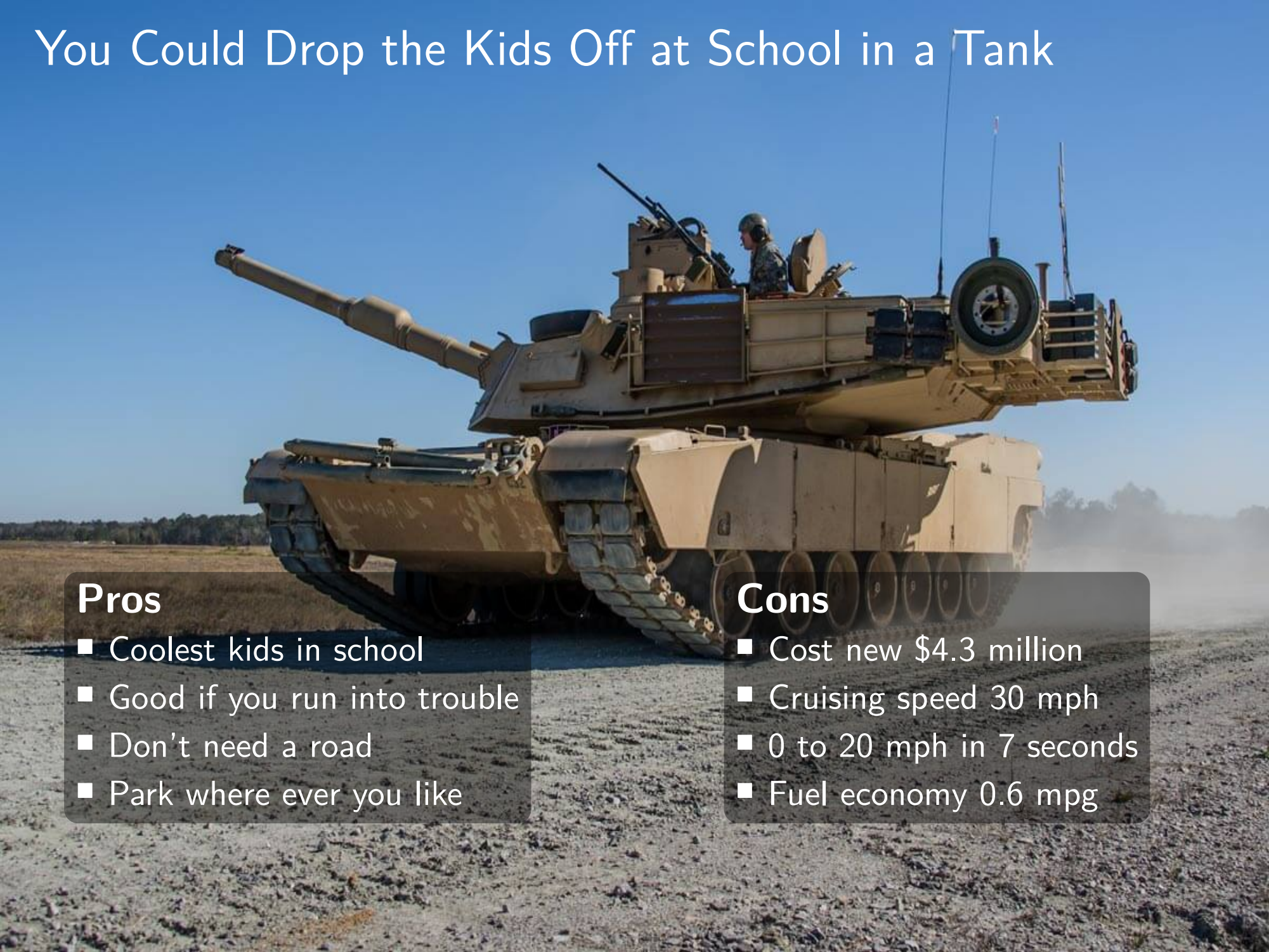
You Could Drop the Kids Off at School in a Tank



Pros

- Coolest kids in school
- Good if you run into trouble
- Don't need a road
- Park where ever you like

You Could Drop the Kids Off at School in a Tank



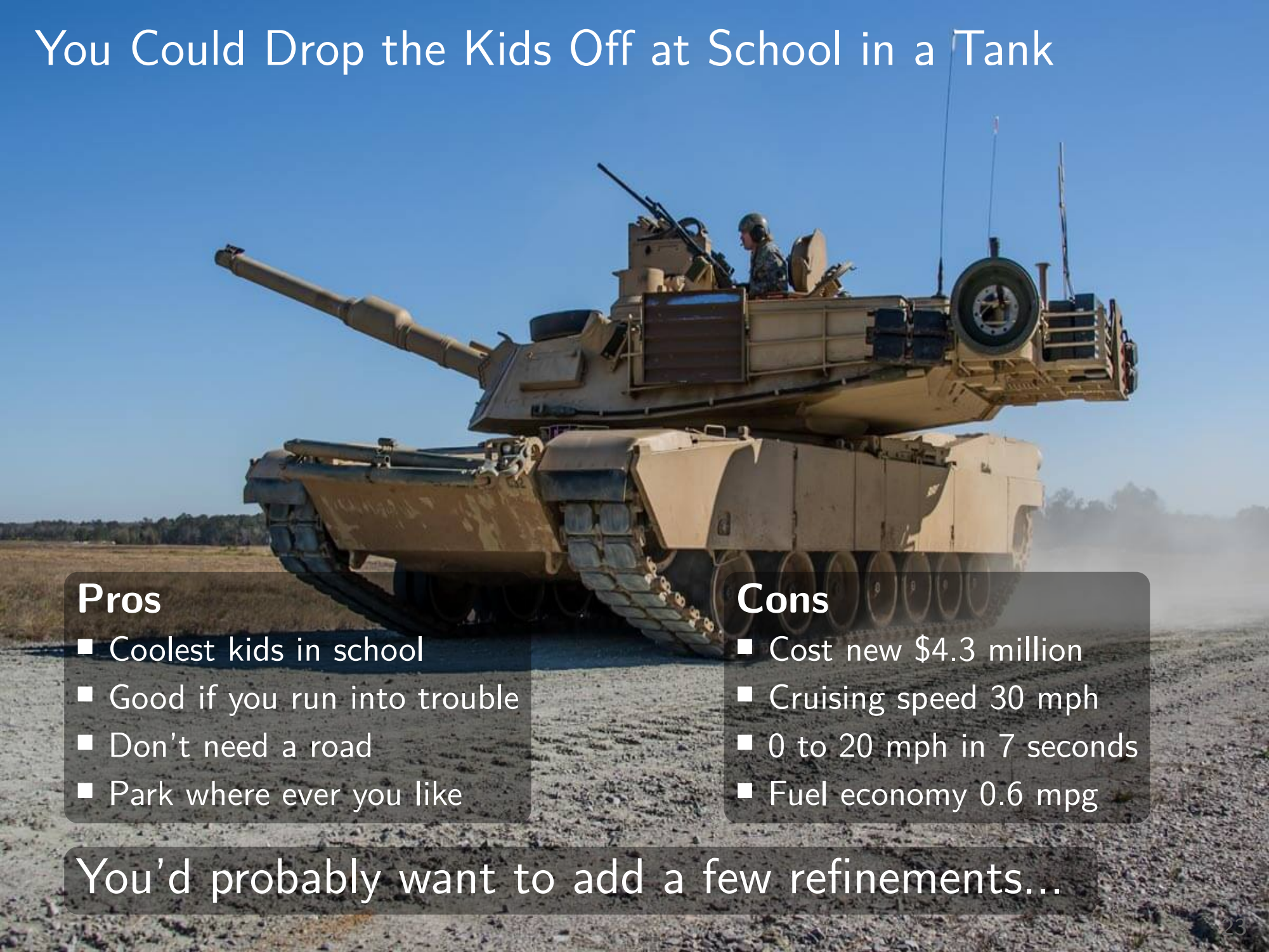
Pros

- Coolest kids in school
- Good if you run into trouble
- Don't need a road
- Park where ever you like

Cons

- Cost new $4.3 million
- Cruising speed 30 mph
- 0 to 20 mph in 7 seconds
- Fuel economy 0.6 mpg

You Could Drop the Kids Off at School in a Tank



Pros

- Coolest kids in school
- Good if you run into trouble
- Don't need a road
- Park where ever you like

Cons

- Cost new $4.3 million
- Cruising speed 30 mph
- 0 to 20 mph in 7 seconds
- Fuel economy 0.6 mpg

You'd probably want to add a few refinements...

...and you'd likely end up with a...

...SQL database

Capabilities and Refinements Are In Conflict

Between	**and**	there is a Conflict
Obvious TTP	Blockchain	Trusted third party administers SQL DB
Public	Permissioned	Coordinate without blockchain
Open source	Governance	Uncoordinated open network = forks
Privacy	Verifiability	Information needed to verify transactions
Trust	Performance	Low/no trust = poor performance
Access	Efficiency	Guaranteed access, distributed = expensive
PII	Public	Expectation of privacy
PII	Immutable	GDPR Right to be forgotten
Me	Everyone else	**Coordination** or **technology** problem?

Capabilities and Refinements Are In Conflict

Between	**and**	there is a Conflict
Obvious TTP	Blockchain	Trusted third party administers SQL DB
Public	Permissioned	Coordinate without blockchain
Open source	Governance	Uncoordinated open network = forks
Privacy	Verifiability	Information needed to verify transactions
Trust	Performance	Low/no trust = poor performance
Access	Efficiency	Guaranteed access, distributed = expensive
PII	Public	Expectation of privacy
PII	Immutable	GDPR Right to be forgotten
Me	Everyone else	**Coordination** or **technology** problem?

- Confidential transactions use zero-knowledge proofs to keep the amount and type of assets transferred visible only to participants in the transaction, while still cryptographically guaranteeing that no more coins can be spent than are available

Insurance Applications

Blockchain Applications

Industry Consortia and Alliances

- AAIS: openIDL = open Insurance Data Link, regulatory data reporting
- R3: distributed ledger, banking; created Corda
- B3i: blockchain Insurance Industry Initiative (London)
- RiskBlock Alliance (The Institutes)

Commercial

- Etherisc: travel and other insurances on Ethereum (Oracle)
- Everledger: registry for diamonds and other real assets (Identity)
- NodalBlock: customer on-boarding, document commitment (Identity)
- Alastria: national blockchain system

B3i Property Cat XOL Contract

Rather than maintain data on separate ledgers of each contracting party (cedent, broker, reinsurer), the B3i blockchain application runs a shared process, calculation, settlement and reporting on a distributed ledger.

- Privacy: Hyperledger manages encrypted information between parties
- Smart contracts drive settlement and asset transfers
- Approvals: digital signatures have their own root of trust without relying on a central authority

Comments

A great technology company should have proprietary technology an **order of magnitude** *better than its nearest substitute. . . . merely incremental improvements often end up meaning no improvement at all*

Thiel, Peter. Zero to One

RiskBlock Proofs of Concept

Use Case	Objectives
Proof of Insurance	Establish electronic safekeeping
	Enable automatic information updating
Subrogation	Facilitate netting of payments
	Optimize costs and streamline processes
Parametric Insurance	Expand parametric insurance
	Automate assessments and payments
First Notice of Loss	Optimize information flow
	Facilitate efficient data sharing
Claims Processing	Automate back office with smart contracts

Comments

- Netting, automation generally **Oracle** problems
- Proof of insurance, subrogation and FNOL are **identity** problems

evernym

Self-sovereign identity: now that it's possible, it's inevitable.

Humanity deserves digital identity that is permanent, portable, private and completely secure; in other words: self-sovereign.

Shortcomings in the internet's original design made this impossible, at a cost of trillions each year. Today, the invention of distributed ledger technology makes self-sovereign digital identity a possibility for the first time.

Now that self-sovereign identity is possible, it's inevitable. And it's going to change everything.

Your Identity in a Tank is the Killer App

Characteristics of identity align with blockchain capabilities

- Permanent = Immutable
- Resolvable = Available, Distributed
- Decentralized = Public Issuance, No Authority
- Verifiable credentials = cryptographic web of trust and an Oracle solution
- Store data on edge devices = no Equifax PII data honey pots
- Explicit user control of data = grant access as needed for each application
- Regulatory compliance = GDPR

Identity Is Central to Insurance

- Individual and corporate identity
  - Link entity to it risk history
  - NCCI experience rating calculations
  - On-boarding insureds
- Tokenization of real assets = physical asset ID
- Proof of insurance
- Contract certainty / commitment = contract ID
- Claim occurrence ID
- Corollary benefit: fraud prevention

Product Concept I

Blockchain (Database) of Claim Occurrence IDs

- Who, what, where, when of each occurrence
- New claims determined ("mined") based on agreed protocol by carriers or third parties
- Ability to merge existing claims, retaining history
- Ecosystem of third-party data augmentation services, e.g. merge police records, weather information
- Subscriber revenue model with reward for mining new occurrence—or ICO for trendy solution
- Permissioned database containing minimal PII and/or encrypted data
- Facilitates claim investigation, subrogation, fraud detection and prevention, underwriting layered and shared (umbrella/excess) policies, excess reinsurance, risk history
- Large existing players ideally positioned to operate and maintain: known and trusted by insurers; acknowledged insurance expertise

Product Concept II

Physical Asset Digital Identity / Tokenization

- Provide self-sovereign ID for physical assets, particularly buildings
- ID created and controlled by owner, hosted on permissioned Blockchain
- ID-linked information created and and maintained by owner and interested third parties with trusted validation, e.g. vendors could merge state and county tax-related data
- Building owner controls release of data
- Service offers easier communication with banks, insurers and other interested parties for renewals and quoting
- Don't create an application from scratch at each renewal!
- Dovetails with businesses in building inspection, fire protection, replacement cost estimates, loss control
- Revenue model: free to create records; charge banks, brokers, insurers for access

Product Concept III

Private Statistical Reporting

- Encrypted statistical reporting
- Receiving statistical agent cannot read data
- Data audited and validated using zero-knowledge proofs
- Adjacent technology to Blockchain
- Regulators provided time-restricted read-only access to data by reporting company
- Target customers: large personal lines companies

Conclusions

Conclusions

Blockchain Pros

- Amazing technical capability—the Internet circa 1995
- Enables unimagined solutions
- Perfect for identity problems

Conclusions

Blockchain Pros

- Amazing technical capability—the Internet circa 1995
- Enables unimagined solutions
- Perfect for identity problems

Blockchain Cons

- Slow, expensive database
- Cyber/real-world interface about ambiguity not smart contracts
- Coordination still required

Coming Soon. . .


WHERE SHOULD WE FOCUS THIS YEAR?
"BLOCKCHAIN"
IT WILL CHANGE EVERYTHING.
EVERYBODY IS TALKING ABOUT IT.
THE POTENTIAL APPLICATIONS ARE ENDLESS.
WE DON'T WANT TO BE LEFT BEHIND.
WHAT EXACTLY IS BLOCKCHAIN?
ALSO, "ARTIFICIAL INTELLIGENCE"
TOM FISH BURNE
©marketoonist.com