Blockchain Mechanics to Insurance Opportunities

Stephen J. Mildenhall, PhD, FCAS, CERA

January 10, 2019

Any sufficiently advanced technology is indistinguishable from magic.

Arthur C. Clarke

Agenda

1. Technical Background
   - Definition
   - Components
   - Identify Real Magic
2. Emergent Capabilities
   - Needs Analysis
3. Applications and Discussion
   - Existing
   - Potential

1. Technical Background

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

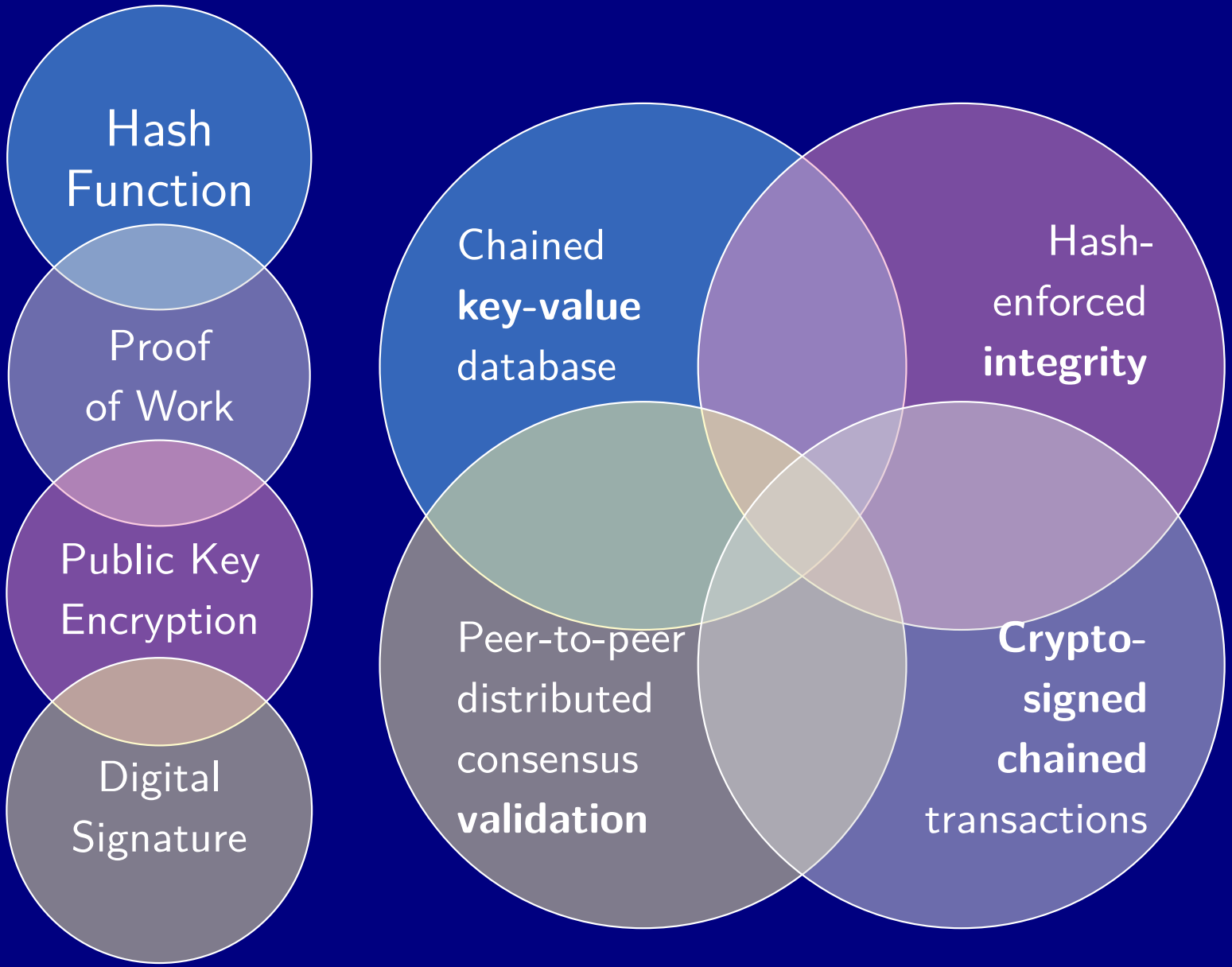
Components

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

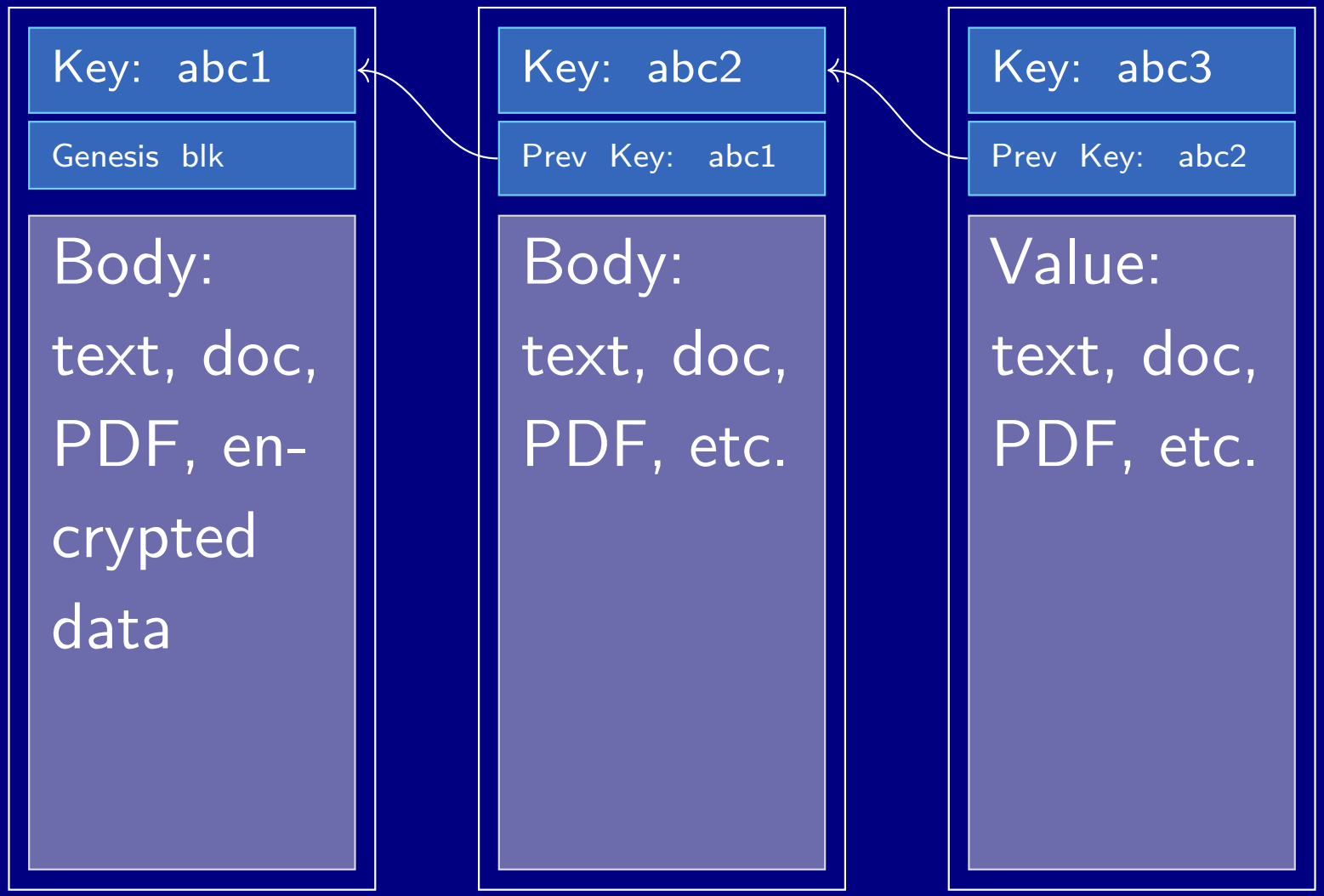
Characteristics

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

Dissect: Magical Ingredients & Recipe



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, ...

Cryptographic Hash Function

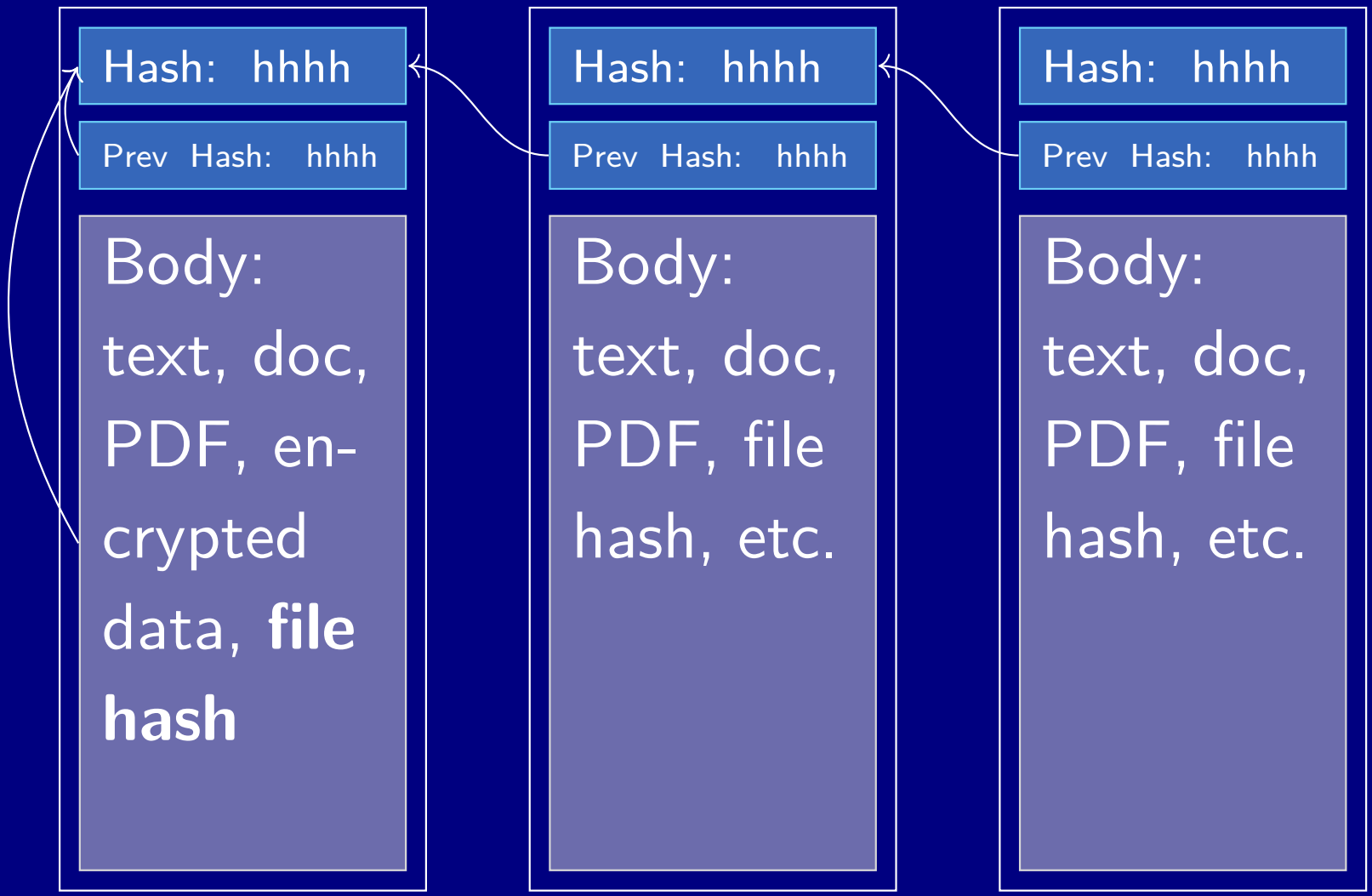
- Given y it is **very hard** to find x with $H(x) = y$
- **Fuggedaboutit** hard

SHA256 Cryptographic Hash Function

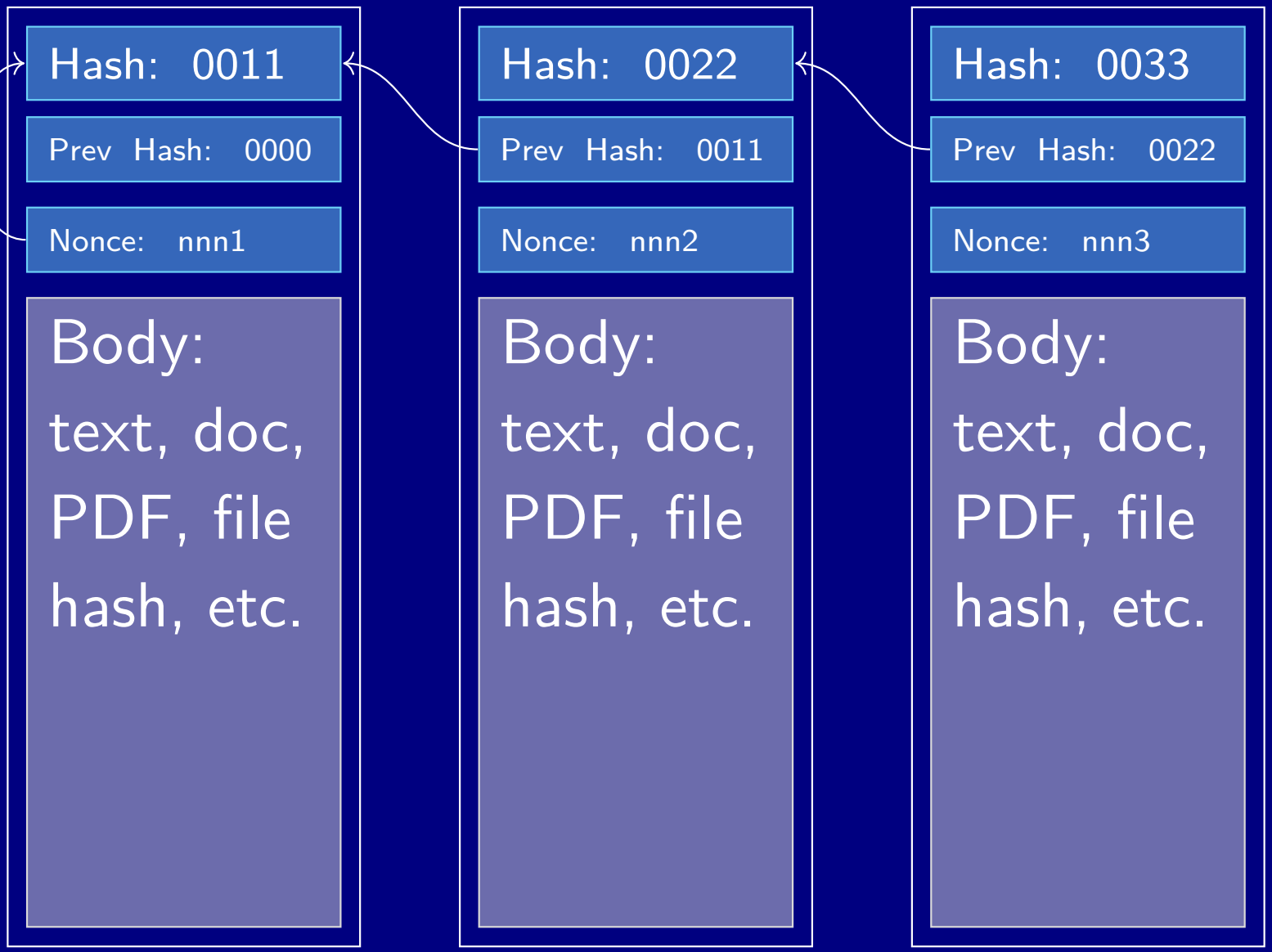
```
import hashlib

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

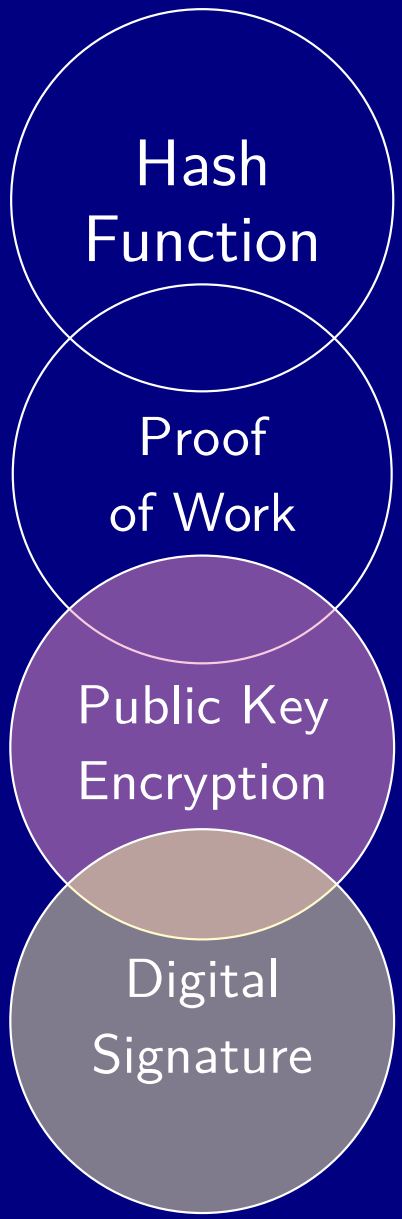
Ingredient 2: Hash-Enforced **Integrity**

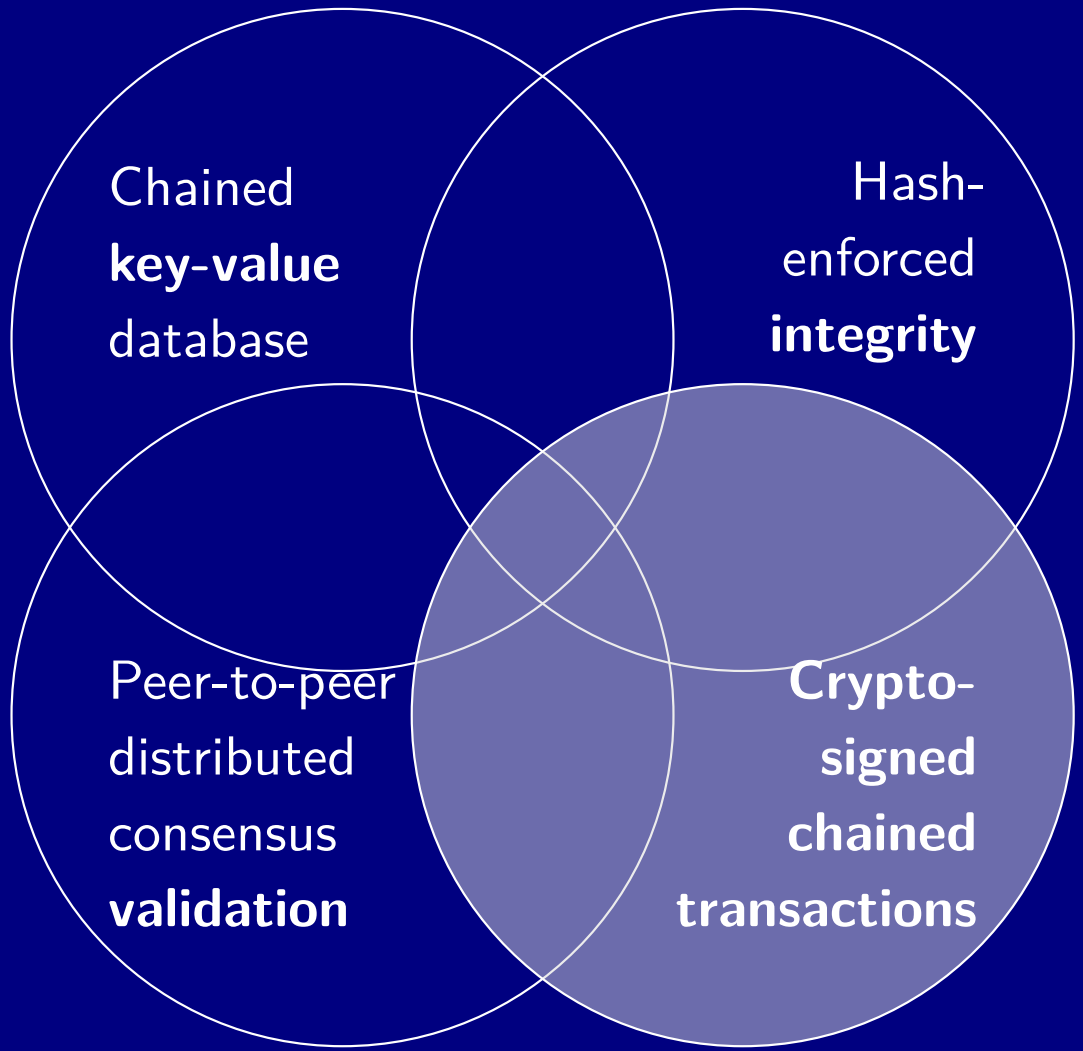


Ingredient 3: Distributed Validation and **Proof-Of-Work**



Dissect: Cryptographic Ingredients





Discrete Logarithm Problem

- **Discrete logarithm problem** says

  given $g^a \equiv n \pmod{p}$ can't find a, the discrete logarithm of g^a

- Discrete logarithm is a one-way function
- Here mod p means remainder after dividing by prime p

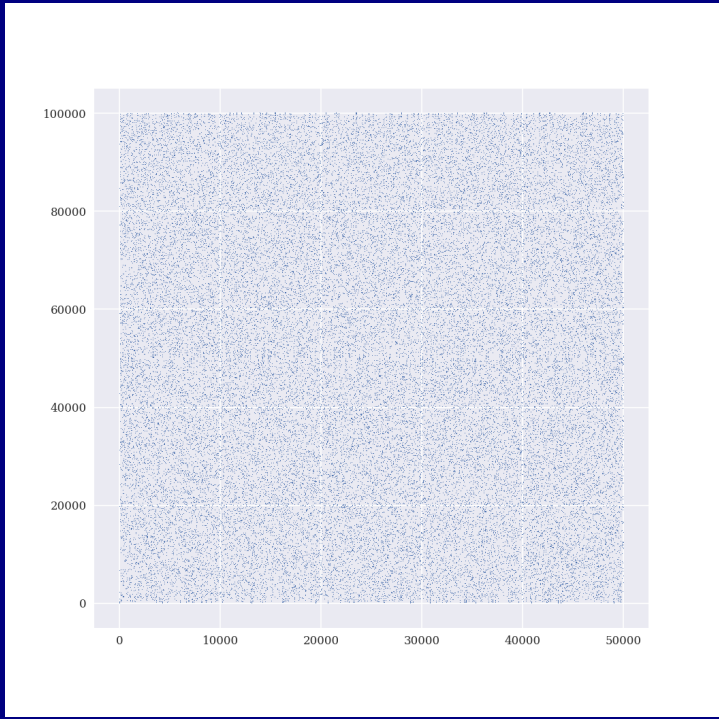
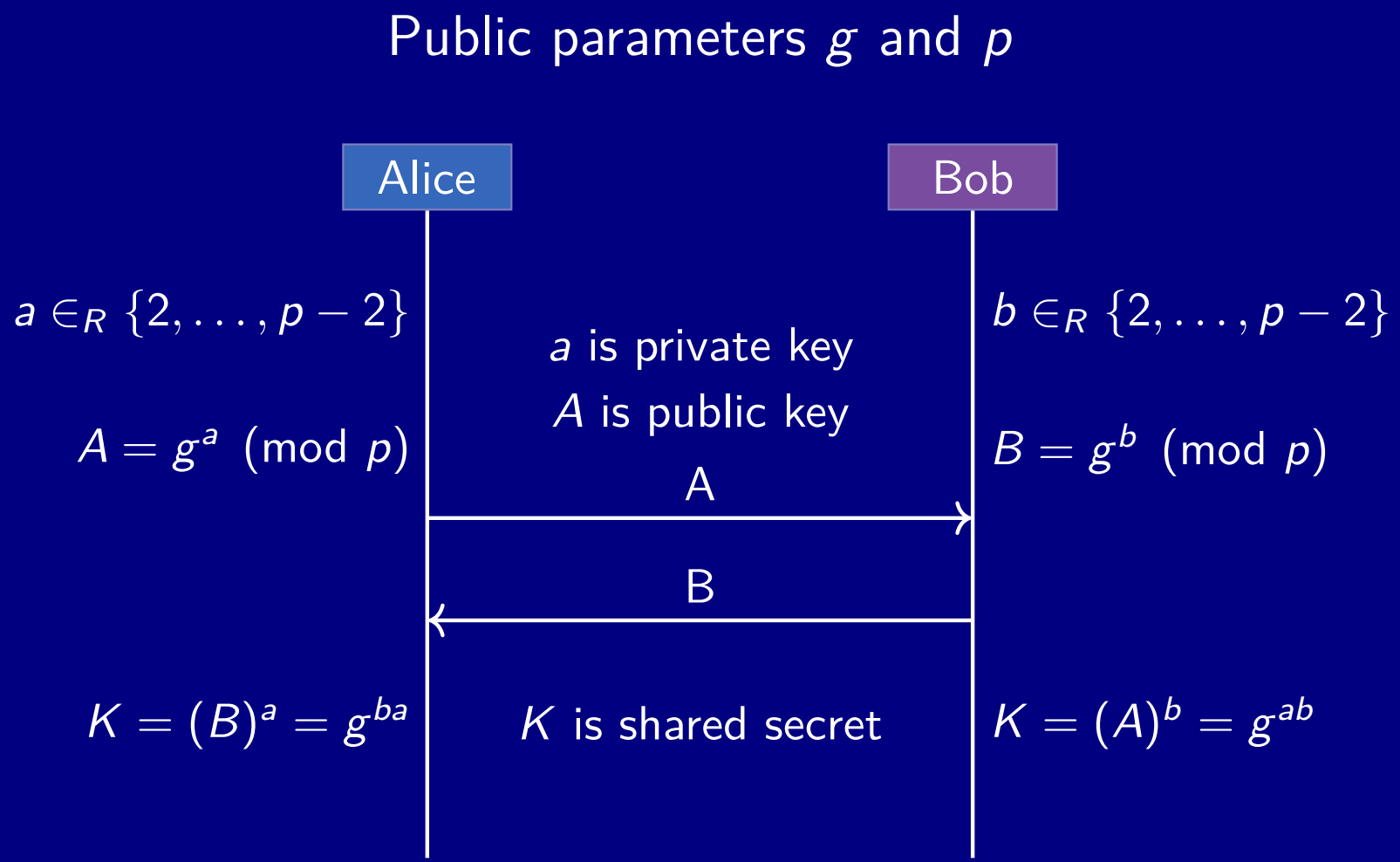


Figure 1: Powers of 3 modulo 100043; 100042 = 2 x 50021 is twice a prime.

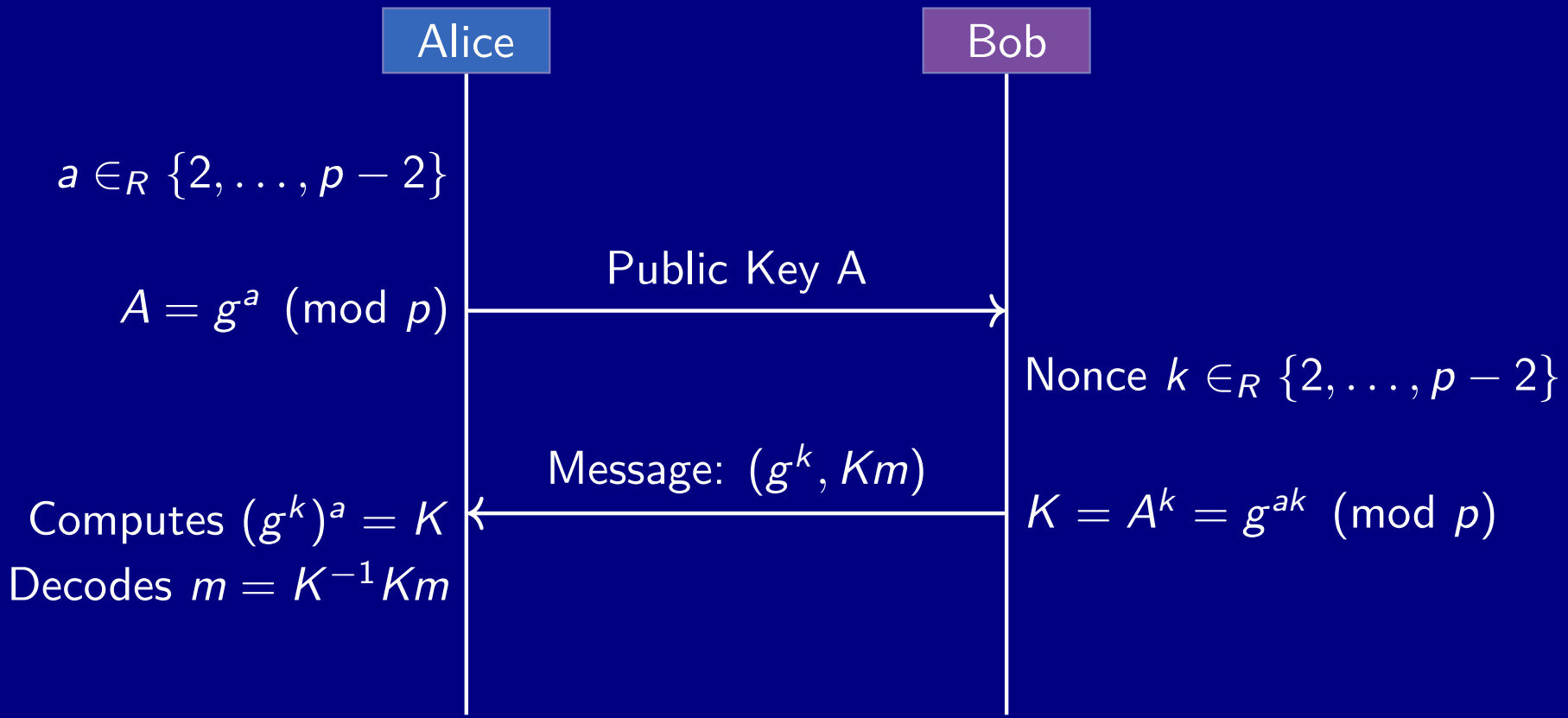
Creating a Shared Secret



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

ElGamel Public Key Encryption

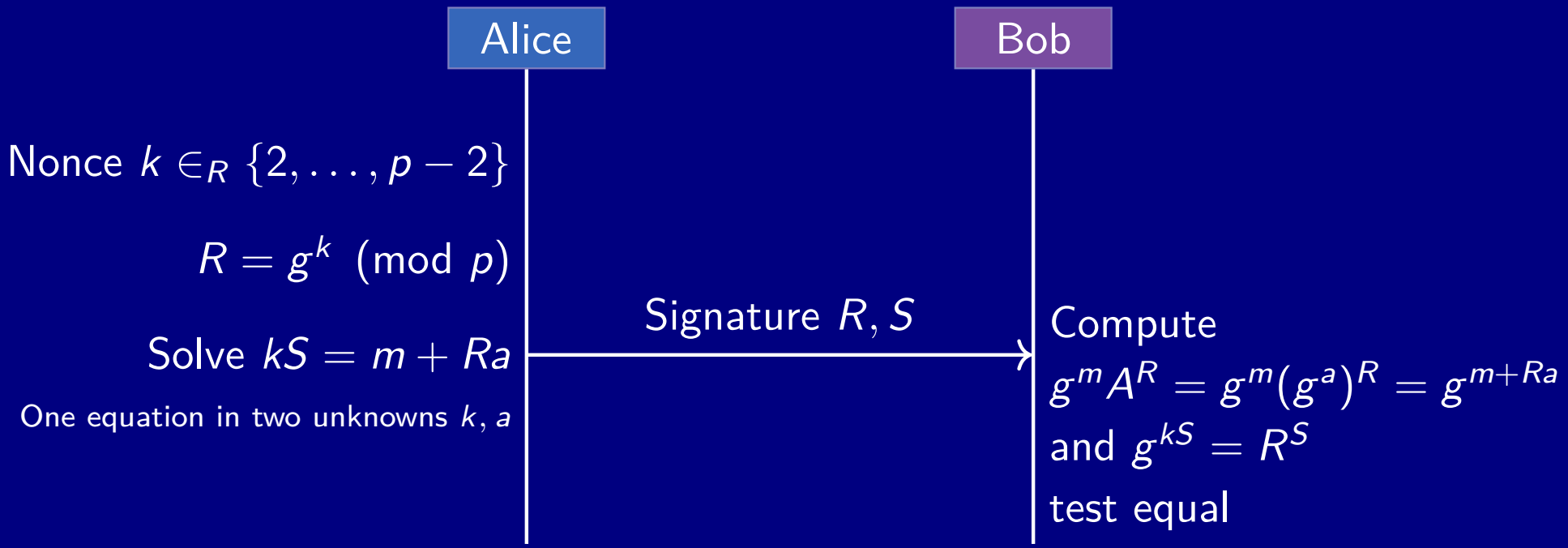
Public parameters g and p
Send message m from Bob to Alice



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



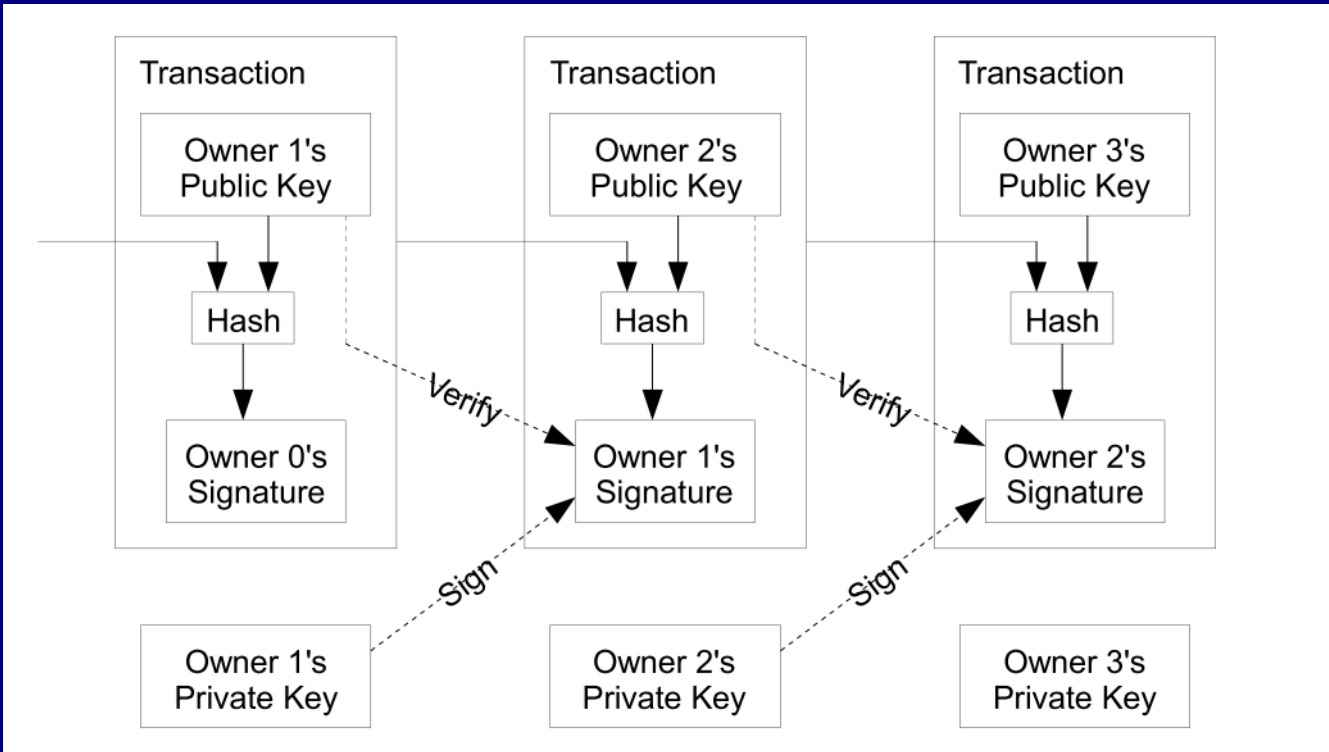
If Alice does not know a she can't find R, S to solve $R^S = g^m A^R$

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

What is a Bitcoin Public Address?

Figure 2: A Bitcoin address is the (double) hash of a public key. It has many different representations.

Adjacent Ingredient: Zero Knowledge Proofs

- It is possible to verify information without revealing it: using a **zero knowledge proof**
- Read-only access, read-act-forget
- Where's Waldo with a mat
- Alibaba's cave

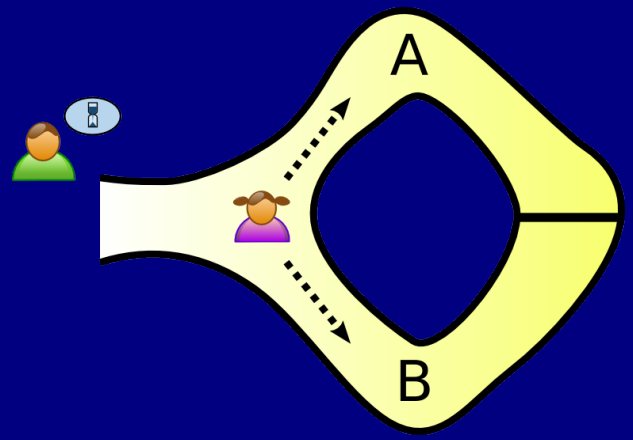


Figure 3: Alibaba's cave example: it is possible to prove you know something without revealing it.

2. Emergent Capabilities

Blockchain: A Solution in Search of a Problem

Using ingredients...

- Hash functions
- Public/private keys
- Digital signatures
- Chained blocks
- Chained transactions
- A clever **incentive**

reinforcing recipe

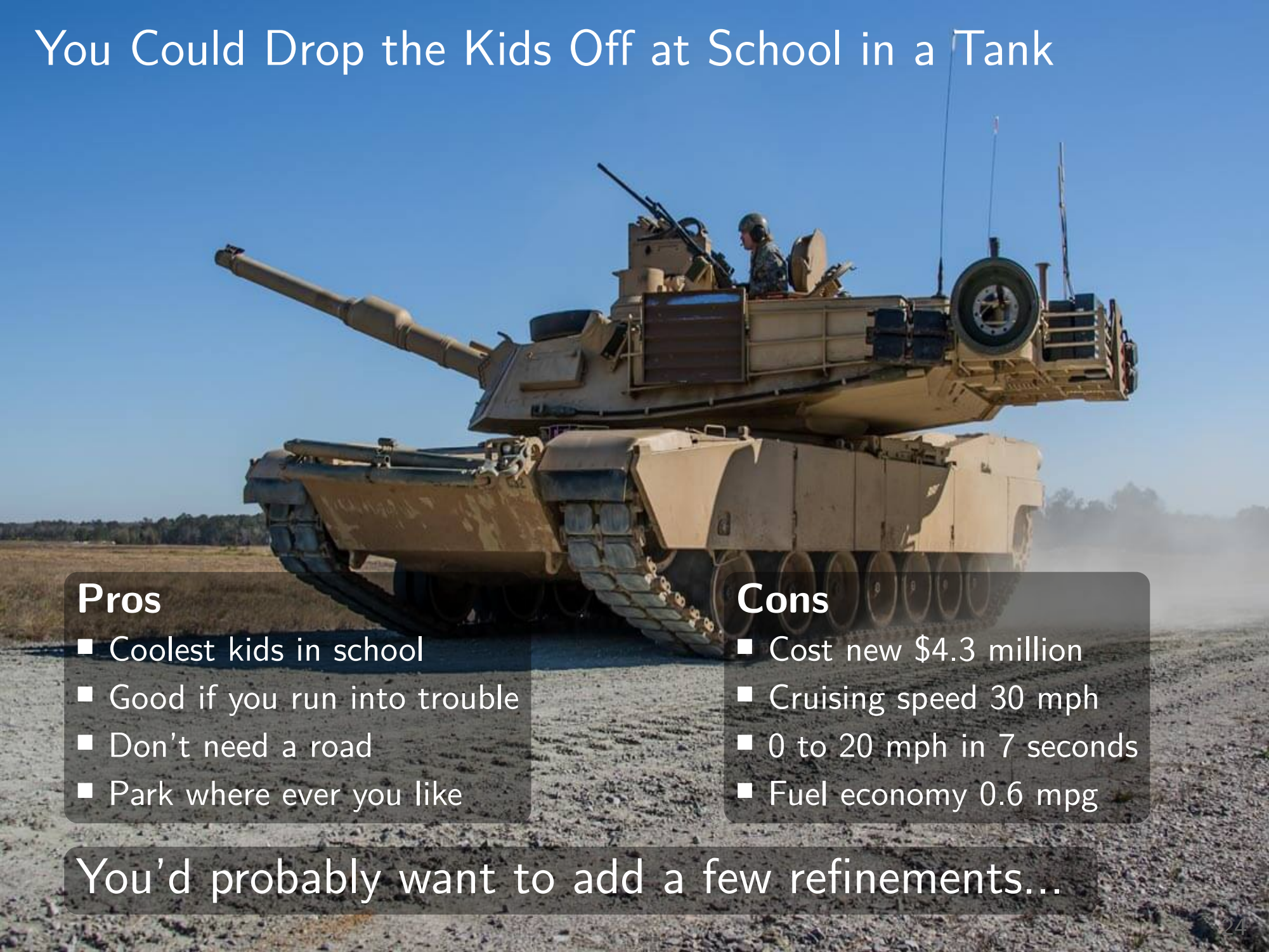
We have created a...

- Distributed...
- Available...
- Public/unsuppressable...
- Immutable database
- No central authority
- Trust between strangers
- Digital scarcity

Applications must **require** these new Blockchain capabilities

- Not just trust = legal contract...
- Not just highly available = DNS, GAFA...
- Not just collaboration = social not technology problem

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...

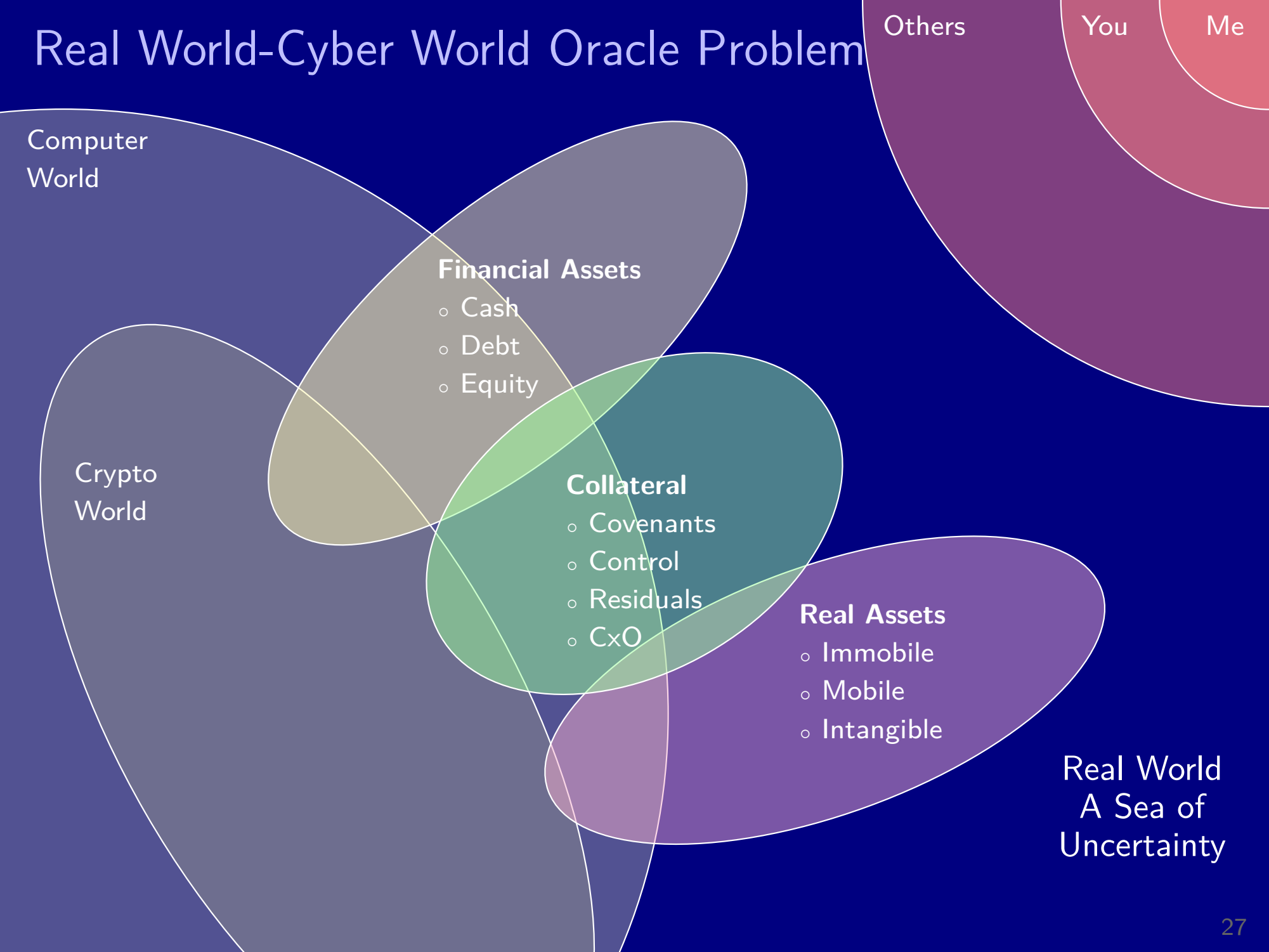
...SQL database

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?

- 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

Real World-Cyber World Oracle Problem



3. Applications and Discussion

Identity is the Killer App

Characteristics of identity align with blockchain capabilities

- Permanent = Immutable
- Resolvable = Available, Distributed
- Decentralized = Public Issuance, No Authority
- You want your identity driving around in a tank
- Google Self-Sovereign Identity and Decentralized Identifiers (DIDs)

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

Identity is the Killer App

Identity solutions leverage blockchain capabilities

- Cryptographically **verifiable credentials** = web of trust and an Oracle solution
- Store data on edge devices and reference with hooks and links stored on Blockchain = no Equifax PII data honey pots
- Explicit user control of data = grant access as needed for each application
- Regulatory compliance = GDPR

Identity is the Killer App

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

Blockchain Applications

Industry Consortia and Alliances

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

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)

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

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

RiskBlock Operational Efficiency Use Cases

Property-Casualty Operations

Blockchain can shorten transaction processing cycles, eliminate paper, streamline interactions with third parties, and provide secure real-time access to data by insurers, distributors and end customers.

Comments

- So can a SQL database with an API
- No solution to Oracle problem (real-world/computer interface)

RiskBlock Operational Efficiency Use Cases

Policy Life-Cycle and Distribution

Blockchain technology will facilitate faster and more efficient quotes and illustrations as well as renewals management through the automation of many previously manual processes.

*Instantly request quotes with the combination of a **digital ID** of the insured and a **digital profile of the asset**. Seamless customer profiling based on digital ID and shared database.*

Comments

- Automation and collaboration; not Blockchain!
- Explicit identity solutions

AAIS openIDL

The openIDL is the first secure, open blockchain platform that enables the efficient and permissioned-based collection of statistical data on behalf of insurance carriers, regulators and other participating contributors.

The openIDL blockchain streamlines the time-consuming and expensive regulatory and compliance requirements carriers experience today, to create operational efficiency, flexibility, interoperability and product development opportunities. The openIDL supports statistical reporting for current and future data calls from regulators, often around emerging or regional exposures or specific events.

Comments

- It's a database
- Data prep is time consuming, not data transmission

AAIS openIDL

With access to timely and accurate information, regulators and reporting carriers receive more holistic and dynamic reporting, as well as valuable and relevant insights into exposures and market trends. Once reports are complete, regulators review and publish the report to the openIDL.

While contributing statistical data to the openIDL Distributed Ledger satisfies regulatory requirements, data remains private and protected from external parties and other openIDL participants. Participating carriers will also see their own data profile to understand how their data compares to the rest of the reporting market.

Comments

- It's an MI system
- It has permissioned roles with controlled data access

AAIS openIDL

As an open blockchain, the openIDL will enable access to new insights from shared experience and input for the development of new products and services and market response and resiliency–not to monetize statistical data. The openIDL will expand with new features and capabilities to support a broad array of use cases by carriers and a growing network of industry partners.

Comments

- To pool or not to pool your data?

B3i Property Cat XOL Contract

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

- Multi-party transactions: cedents, brokers and reinsurers underwriting a contract via nodes;
- Privacy: the Hyperledger architecture channels manages encrypted information between parties;
- Smart contract logic in computational logic: in a property Cat Excess of Loss contract;
- Multi-layers: combining programs, layers, sections and proportional and XOL logic;
- Approvals: our digital signatures have their own root of trust without relying on a central authority;
- Settlement: all common accounting data to settle the contract post-placement are generated;
- Asset transfers: state changes lead to value transfers, traceable in an immutable, digital way.

A great technology company should have proprietary technology an order of magnitude better than its nearest substitute. . . . Companies must strive for ***10x better*** *because merely incremental improvements often end up meaning no improvement at all for the end user. (Thiel, Peter. Zero to One)*

Specific 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
- Verisk ideally positioned to operate and maintain: known and trusted by insurers; acknowledged insurance expertise

Specific Product Concept II

Physical Asset Digital Identity

- 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 Verisk businesses in building inspection, fire protection, replacement cost estimates, loss control
- Revenue model: free to create records; charge banks, brokers, insurers for access

Specific 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

Appendix

Selected References

Slide(s)	Source or Reference
Definition	Blockchain Technology Overview, Yaga et al (2018), NIST, https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf
Digitial Signature	A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, T. ElGamal, HP Labs, 1985
Double Spend	Bitcoin: A Peer to Peer Electronic Cash System, Satoshi Nakamoto (2008) https://bitcoin.org/bitcoin.pdf
Confidential Transactions	Confidential Assets, Andrew Poelstra et al, 2017
Identity	Drummond Reed, Decentralized Identifiers (DIDs) The Fundamental Building Block of Self-Sovereign Identity https://goo.gl/Au4uBx
	"Self-sovereign identity: now that it's possible, it's inevitable", https://www.evernym.com/
RiskBlock	https://www.theinstitutes.org/doc/riskblock/RiskBlock_Toolkit.pdf
AAID openIDL	https://aaisonline.com/aais-openidl
B3i Prop Cat	https://b3i.tech/our-product.html
	Thiel, Peter. Zero to One: Notes on Startups, or How to Build the Future (p. 155). The Crown Publishing Group.