Blockchain: Magic, Mechanics and Methods

Stephen J. Mildenhall

November 28, 2018

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

Blockchain: Magic and Marketing

[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
- ____________________
- ____________________

Universal Solution!

[Your Industry] Blockchain Opportunity Slide

Your Business Problems

Customer Experience
- Confusing products
- High expenses

Your Problem 1
- ____________________
- ____________________

Your Problem 2
- ____________________
- ____________________

Your Problem 3
- ____________________
- ____________________

Universal Solution!

Blockchain delivers...
- Best customer experience
- Immutable record
- Enables collaboration
- One view of truth
- End duplicate 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

- ____________________
- ____________________

Universal Solution!

Blockchain delivers...

- Best customer experience
- Immutable record
- Enables collaboration
- One view of truth
- End duplicate 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

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

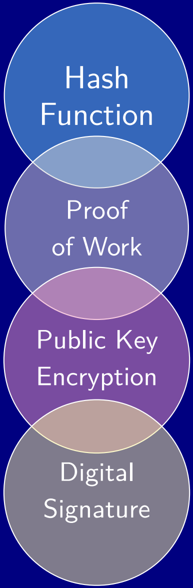
Components

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

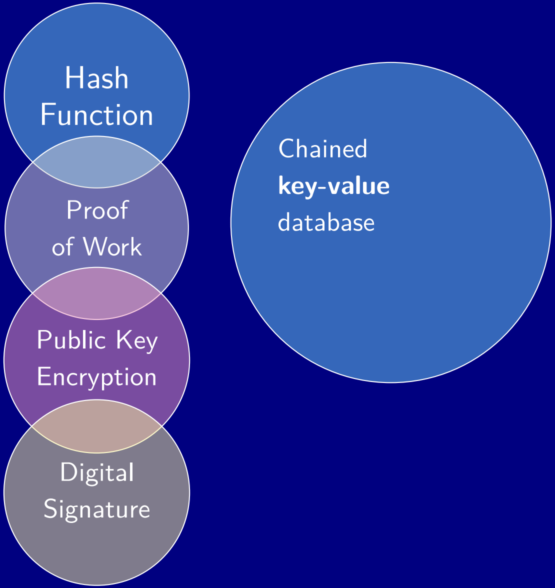
Characteristics

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

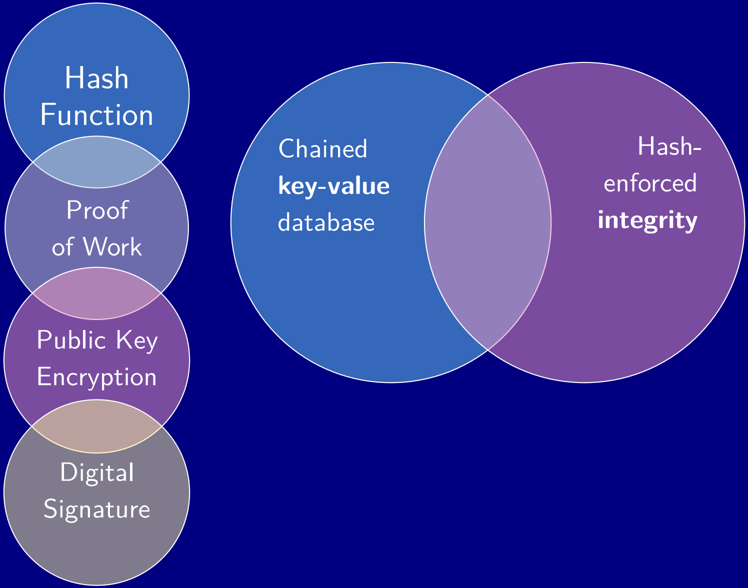
Dissect: Magical Ingredients & Recipe



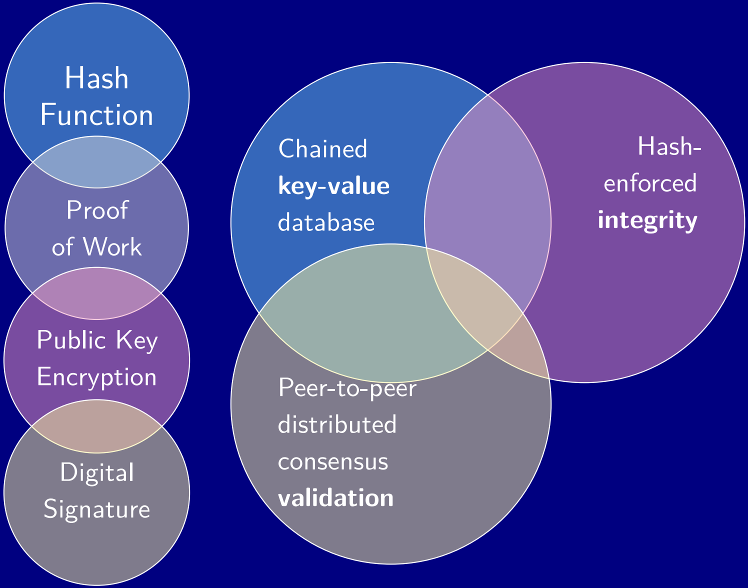
Dissect: Magical Ingredients & Recipe



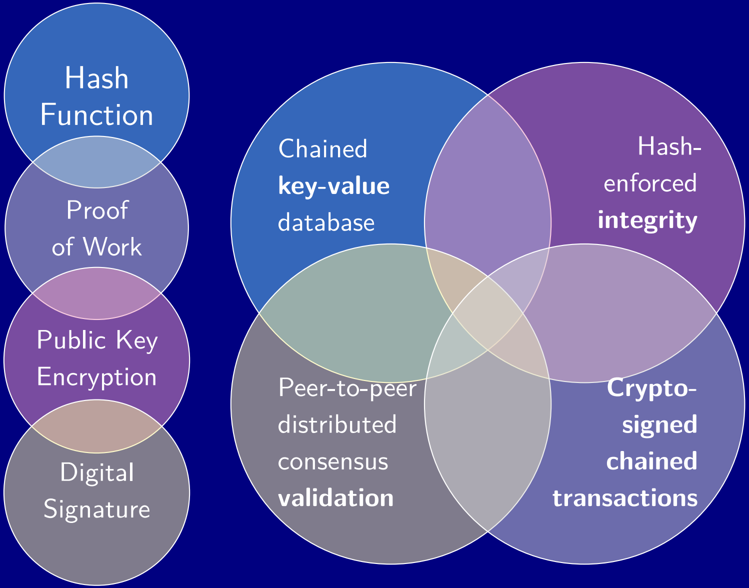
Dissect: Magical Ingredients & Recipe



Dissect: Magical Ingredients & Recipe



Dissect: Magical Ingredients & Recipe

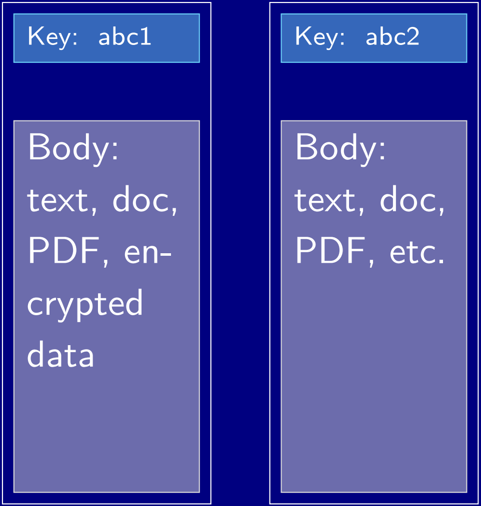


Ingredient 1: Chained Key-Value (Distributed) Database

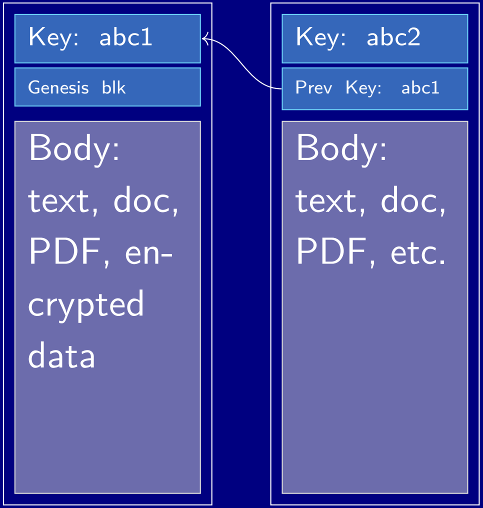
Key: abc1

Body: text, doc, PDF, encrypted data

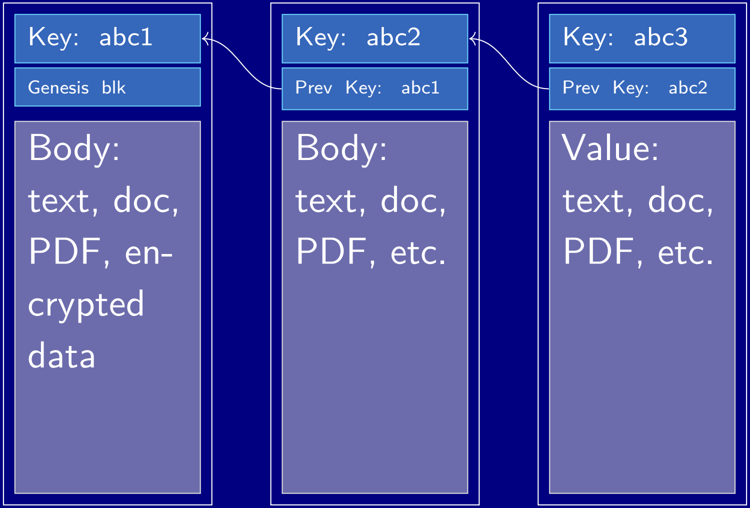
Ingredient 1: Chained Key-Value (Distributed) Database



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, ...

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'
```

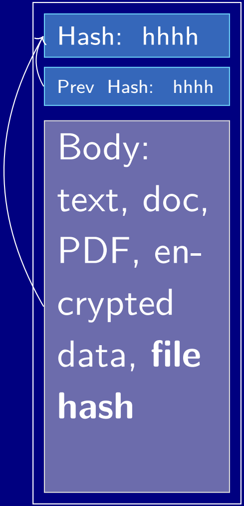
- Output = **very** large integer, between 0 and $2^{256} \approx 10^{77}$
- Specify input and output formats **very carefully**
- Probability of J. Smith collision: not even a Dumb and Dumber chance

The Birthday Problem and Hash Collisions

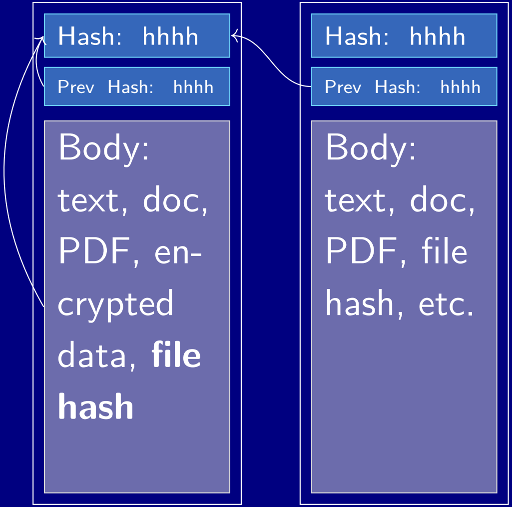
- Birthday problem: 23 people for 50/50 chance of same birthday
- Number of documents before p probability of collision given a hash space size of N is $\approx \sqrt{2Np}$ for small p[1]
- For SHA256, $N = 2^{256} = 10^{77}$ is very large
- A 10^{-3} collision probability requires about 1.5×10^{37} documents, enough for
  - Every person on earth to...
  - Compute 1 billion hashes per second...
  - For five times the age of the universe

[1] E.g. for birthday problem $p = 1/2$, $N = 365$ and $\sqrt{2Np} = 19$. Approximation relies on $p \approx -\log(1-p)$, only true for smaller p. Using $(-2N\log(1-p))^{1/2} = 22.49$ is very close to correct answer, 23.

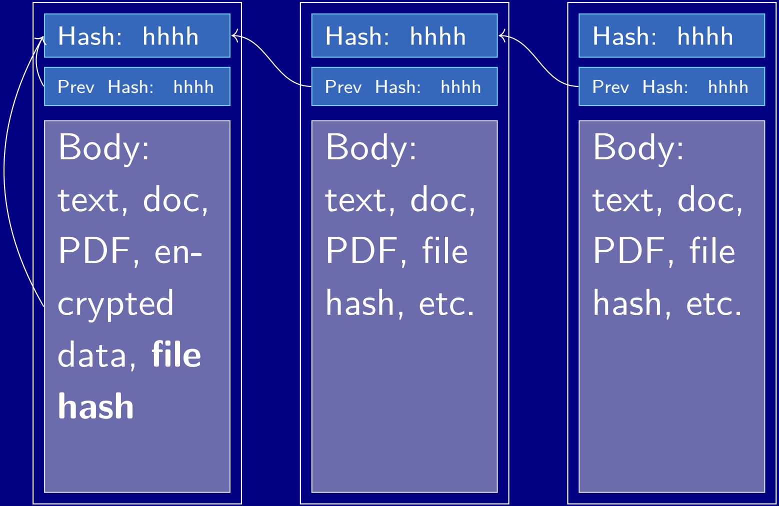
Ingredient 2: Hash-Enforced **Integrity**



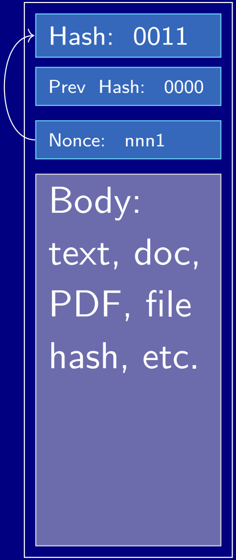
Ingredient 2: Hash-Enforced **Integrity**



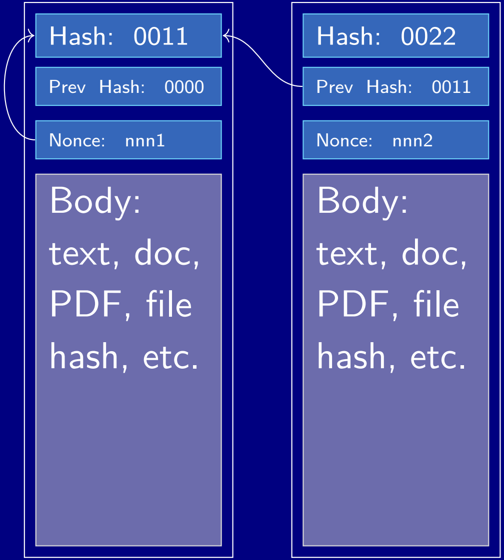
Ingredient 2: Hash-Enforced **Integrity**



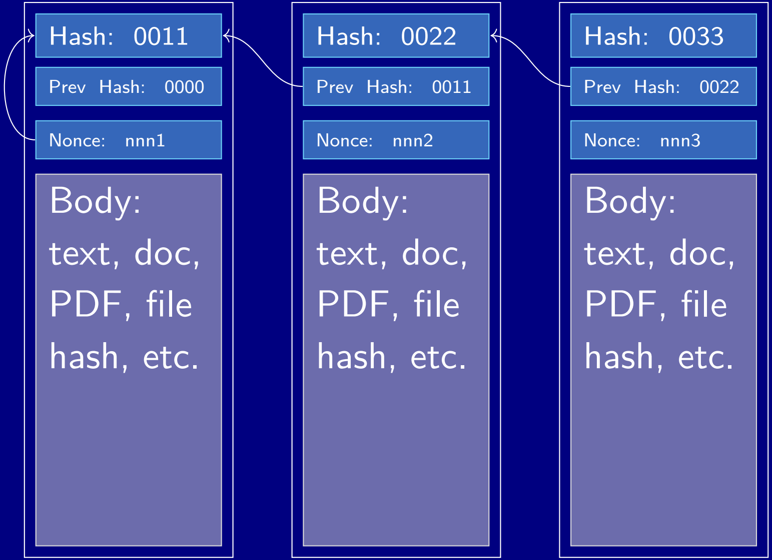
Ingredient 3: Distributed Validation and **Proof-Of-Work**



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



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



Proof of Work and Bitcoin Mining = Compute Hashes

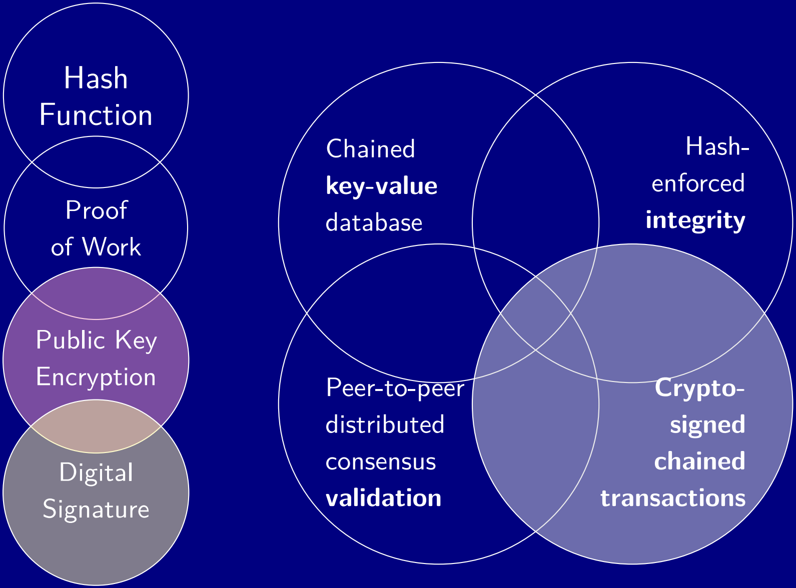
```
import hashlib

running_min = 2**256
ans = []
base = b'The quick brown fox jumps over the lazy dog'

for nonce in range(2000000000):  # 2 billion
    h = hashlib.sha256(nonce.to_bytes(4, byteorder='big') + base).hexdigest()
    n = int(h, 16)
    if n <  running_min:
        running_min = n
        ans.append([nonce, n])
        print(f'{nonce:12,d}   {n:077}')
```

Proof of Work and Bitcoin Mining = Compute Hashes

Nonce	Hash
0	29115579230639891023898657467946481563928575965694753738500728003067276450760
3	21833633896494697913657452817095065461049276120751755746016193921330837964982
8	17391853960576662285627567225372501697536440120814058733709287576654299269058
9	00 4917416733711715700273679963357367846227913200158937725721999780085406147 86
817	00 2071131484845376181446046634164375894402892733190271166712540330656434191 32
827	000 350296508952917147540471206794929279682506549018178174340812419369873617 35
3,292	000 305902948951234584937028915270699754429715518755668050227726710842649197 45
6,362	000 231570069085552320189038798777540513152198963226613050996062531437744887 85
7,634	000 118430950735229944225612747208573169310667194863825506155731714048799219 66
22,034	0000 60451607644651032561548150459926799303602226155507667798244523886549846 39
32,737	0000 32187180107165168072460236389190322026739879694343844301662151051322805 83
43,078	0000 30669403671112770877983947657844805132277888309725801175415054188909487 12
50,740	00000 3448040051944983924733628481347618311343044532028751737591302161056190 80
260,109	00000 1490431228082370323455618729051332160604673843699105931139979650626023 36
610,827	000000 254412049392687654201559176987358403434968096869694510426876511327776 55
3,553,698	000000 123725859849952380230815340310268087914547619191394756655490302595930 11
16,603,005	0000000 46823087924447396131193161550339860672825873568639790135107802846114 82
45,767,445	0000000 42951358104398079390374875634099665781087552299396055984855946945002 74
56,389,936	0000000 12198905539705110106931604590869140396900752658626777240488177414064 04
186,599,009	00000000 7417333989151758141116791601595623296416668495351522123102551582837 08
187,060,155	00000000 1290279769730686785541364182372683207087908396263167601734440802355 51
209,437,773	000000000 464187921929729776227088786427802262805389774821319160770981536886 58
554,751,705	000000000 384920570035170526076009189693101063714823161382308355784044605559 13
1,724,412,865	000000000 209514119548306775381123386581050963598131682324527402776756027775 90

- Current network hash rate 4×10^{19} hashes per second
- Electricity consumption = Austria
- Block hash: 0x 0000 0000 0000 0000 0051 a841 86ab c5df . . . .

Dissect: Cryptographic Ingredients



Discrete Logarithm Problem

- **Discrete logarithm problem** says

$$\text{given } g^a \equiv n \pmod{p} \text{ can't find } a$$

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

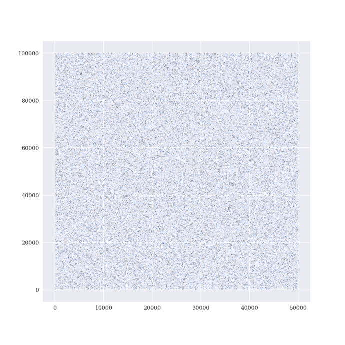
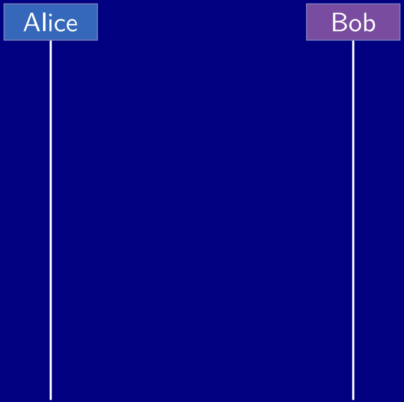


Figure 1: Powers of 3 modulo 100043; 100042 = 2 x 50021 is twice a prime.

Creating a Shared Secret

Public parameters g and p



Creating a Shared Secret

Public parameters g and p

Alice

Bob

$a \in_R \{2, \ldots, p-2\}$

$A = g^a \pmod{p}$

a is private key

A is public key

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

Creating a Shared Secret

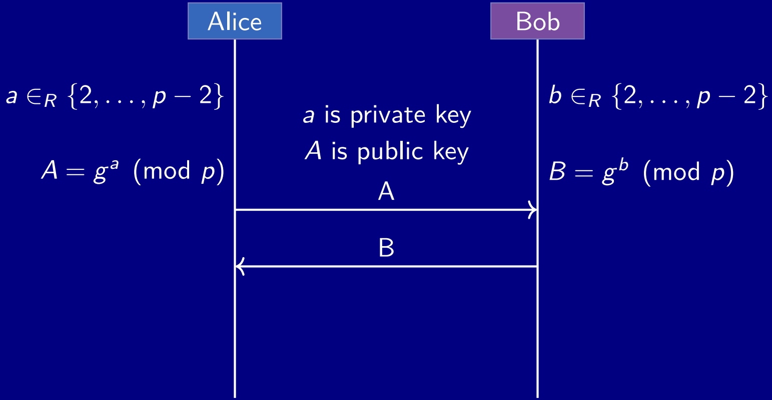
Public parameters g and p

Alice		Bob
$a \in_R \{2, \ldots, p-2\}$	a is private key	$b \in_R \{2, \ldots, p-2\}$
$A = g^a \pmod{p}$	A is public key	$B = g^b \pmod{p}$

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

Creating a Shared Secret

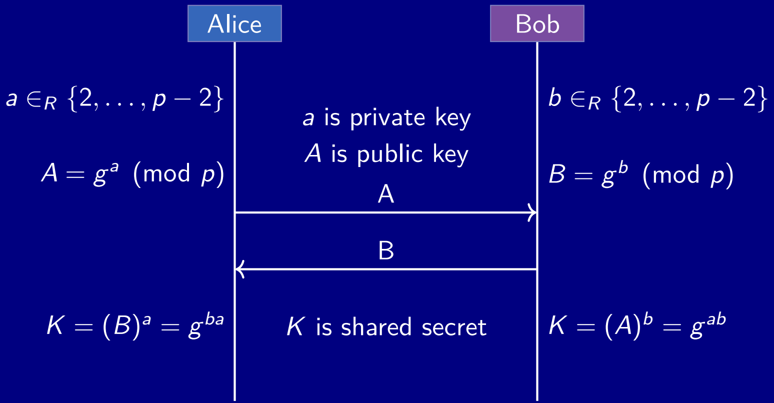
Public parameters g and p



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

Creating a Shared Secret

Public parameters g and p

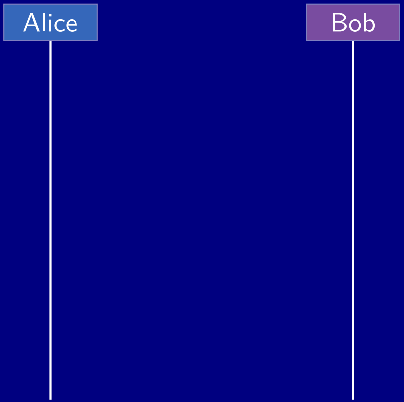


Public/private pair (A, a) are cryptographically linked but a is hidden

ElGamel Public Key Encryption

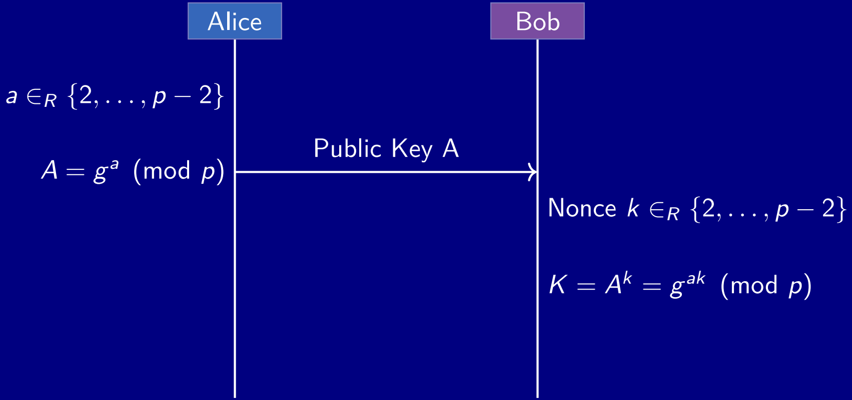
Public parameters g and p

Send message m from Bob to Alice



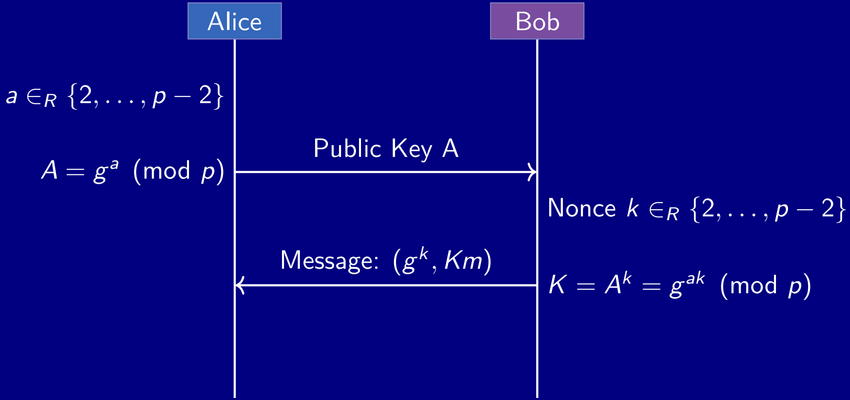
ElGamel Public Key Encryption

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



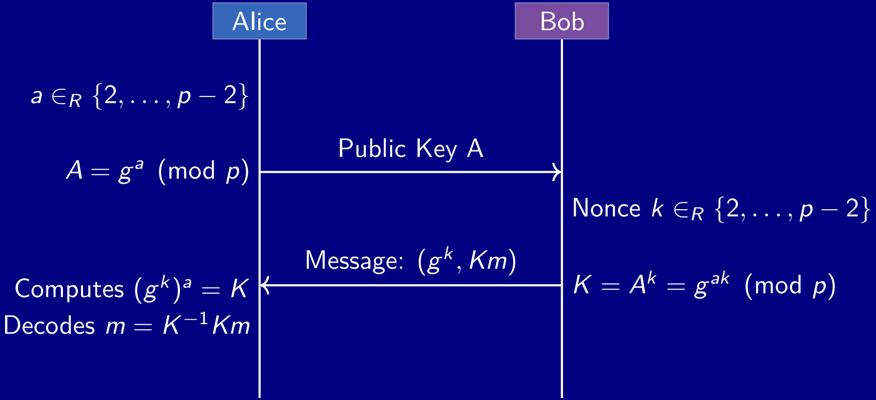
ElGamel Public Key Encryption

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

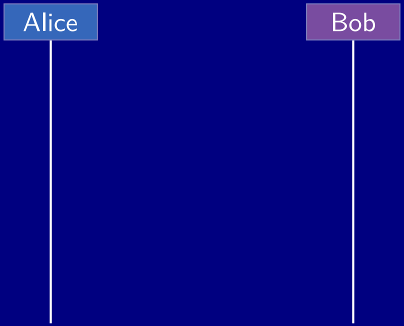


g^k conveys information about k but shields its value; K hides message m

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

Alice

Bob

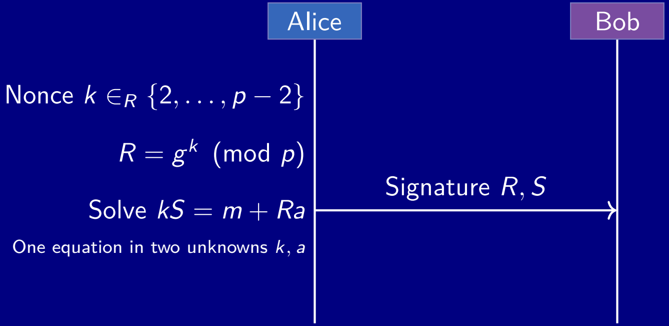
Nonce $k \in_R \{2, \ldots, p-2\}$

$R = g^k \pmod{p}$

Solve $kS = m + Ra$

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

Alice → **Bob**

Alice:

Nonce $k \in_R \{2, \ldots, p-2\}$

$R = g^k \pmod{p}$

Solve $kS = m + Ra$

One equation in two unknowns k, a

Alice → Bob: Signature R, S

Bob:

Compute

$g^m A^R = g^m (g^a)^R = g^{m+Ra}$

and $g^{kS} = R^S$

test equal

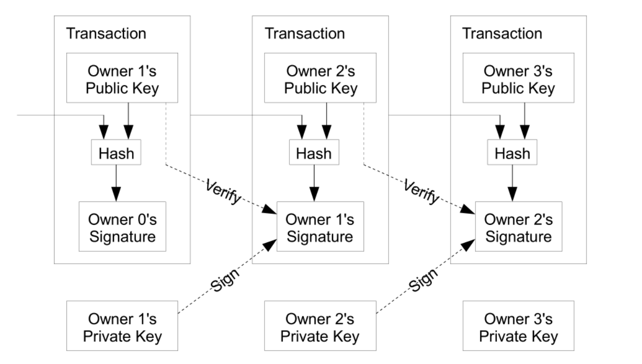
If Alice does not know a she can't find R, S to solve $R^S \; = \; g^m A^R$

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



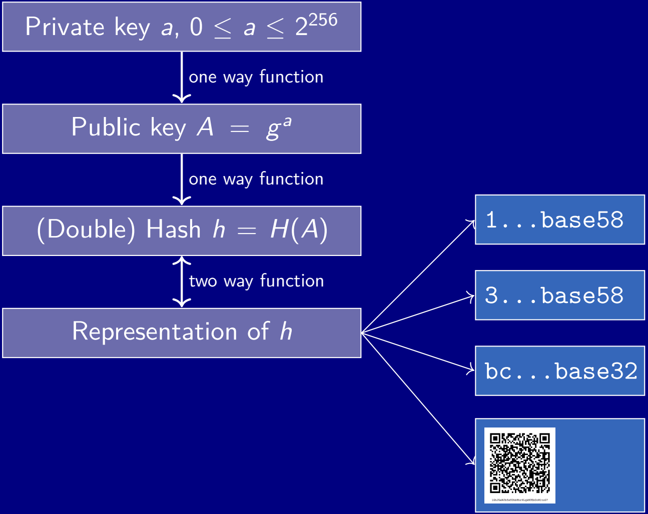
Bitcoin: A Peer to Peer Electronic Cash System, Satoshi Nakamoto (2008) https://bitcoin.org/bitcoin.pdf

What is a Bitcoin Public Address?

1GhJGaWJbSsSDhbHhr9LqkMUEbDoW1tzG7

Figure 2: Donations gratefully received.

What is a Bitcoin Public Address?



What is a Bitcoin Public Address?

If You Know What You Are Doing...

Load into Bitcoin Core Client and get addresses via WIF compressed representation of private key

```
importprivkey
  L5F6PZo9h2RJnGGvztwWEUnwYH1eWhpv63Z5qQEZgqxcy364nBCQj
  yourName

getaddressesbyaccount yourName

[
  "12mvf9RwaQx7XTk4cfN4j4XbVYqfoFh7W5",
  "3HW2VY23bx3RZgBUKxWnwfS26n1Cm2eUaq",
  "bc1qzdmnsg599gc88kg4arraaeg4sy9cdpkd3k3kep"
]
```

Discovery: 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

Must discover applications requiring new features...

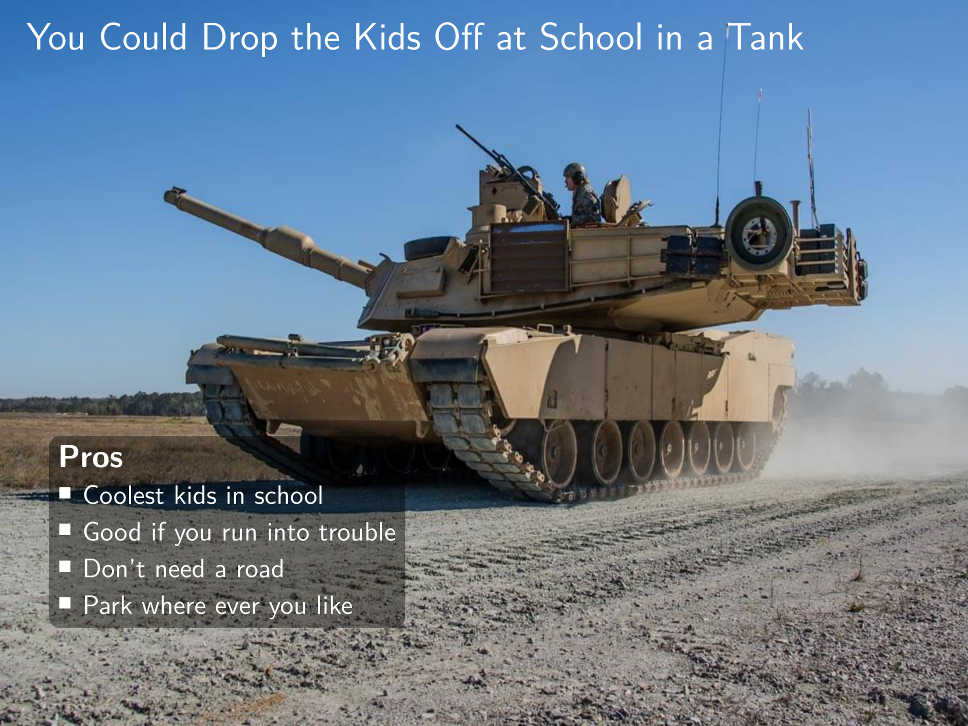
not just trust = legal contract...

not just highly available = DNS, GAFA...

we've built a tank of the database world...

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

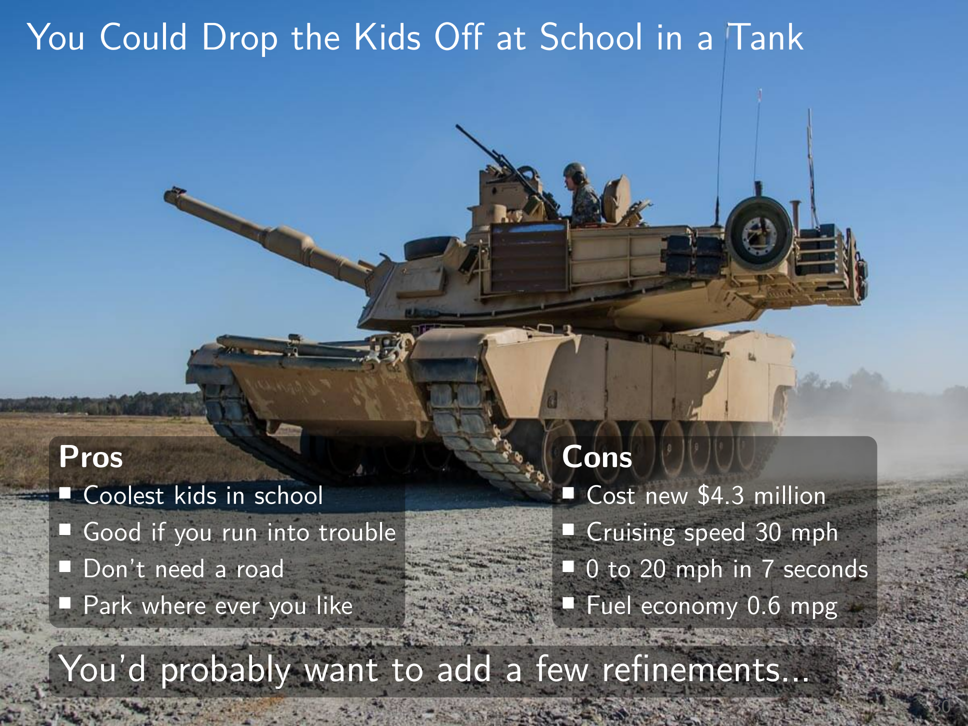
Pros

- 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 can keep the amount and type of assets transferred visible only to participants in the transaction (and those they choose to reveal the blinding key to), while still cryptographically guaranteeing that no more coins can be spent than are available 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.

Identity is the Killer App

Self-Sovereign Identity and Decentralized Identifiers (DIDs)

- Permanent
- Resolvable
- Cryptographically Verifiable
- Decentralized
- Verifiable credentials
- Store data on edge devices, no central stores of PII
- User control of own data
- GDPR

Drummond Reed, Decentralized Identifiers (DIDs) The Fundamental Building Block of Self-Sovereign Identity https://goo.gl/Au4uBx

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

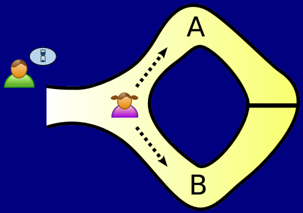


Figure 3: Alibaba's cave example: it is possible to prove you know something without revealing it.

InsureTech Blockchain Applications

Industry Consortia and Alliances

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

InsureTech Blockchain Applications

Industry Consortia and Alliances

- R3: distributed ledger, banking; created Corda
- RiskBlock Alliance (The Institutes)
- B3i: blockchain Insurance Industry Initiative (London)
- AAIS: openIDL = open Insurance Data Link, regulatory data reporting
- Alastria national blockchain system
- **Cooperation and coordination is a social problem not a technology problem!**

InsureTech Blockchain Applications

Commercial Solutions

- Etherisc: travel and other insurances on Ethereum
- Everledger: registry for diamonds and other real assets, an **identity** solution
- NodalBlock: customer on-boarding, document commitment

InsureTech Blockchain Applications

Deployment Options

- Ethereum network smart contract, "world computer"
- Bitcoin network, did:btcr, Lightning network
- Hyperledger
- Corda open-source DLT/blockchain platform
- Private forks of open source solutions

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