Blockchain: An Introduction

Jake van der Laan
Director, Information Technology and Regulatory Informatics,
Chief Information Officer
Financial and Consumer Services Commission
New Brunswick, Canada
jake.vanderlaan@fcnb.ca
https://www.linkedin.com/in/jakevanderlaan/

FUTURE OF PRIVACY FORUM

Any opinions expressed are my own and do not necessarily reflect the position or perspective of FCNB.

I do not endorse, or otherwise make any claim or statement, negative or positive, about any of the websites, companies, or products, if any, referenced in these slides or during this presentation.

FUTURE OF PRIVACY FORUM

Our learning journey today

What a blockchain is and how it works

Types of blockchains

Use case: cryptocurrencies

Blockchain as a “platform”

“Smart contracts”

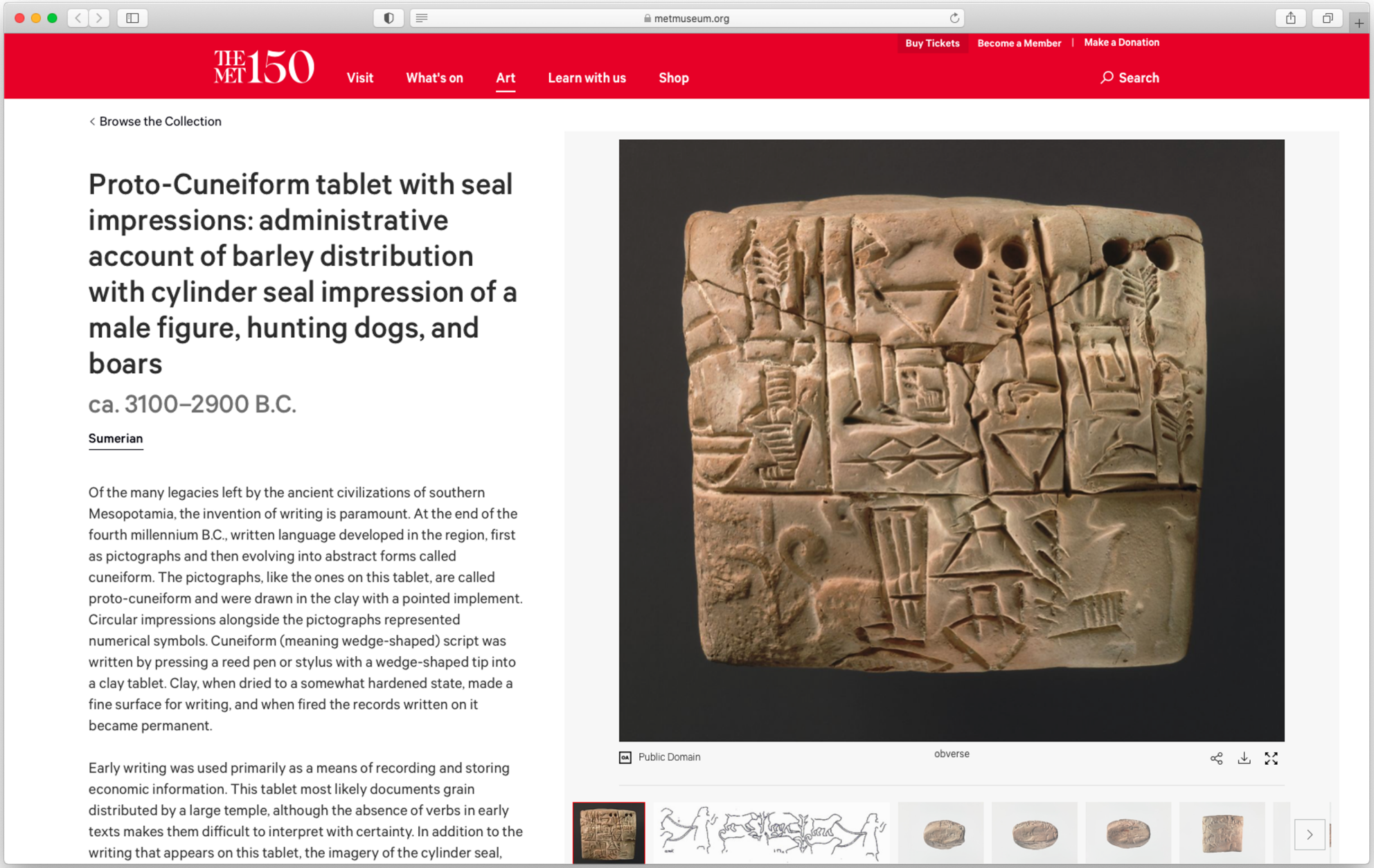
FUTURE OF PRIVACY FORUM

A blockchain in one sentence

An “append only transaction log”

FUTURE OF PRIVACY FORUM

Recordkeeping



FUTURE OF PRIVACY FORUM

FUTURE OF PRIVACY FORUM

FIRST BANK OF WIKI

1425 JAMES ST, PO BOX 4000
VICTORIA BC V8X 3X4 1-800-555-5555

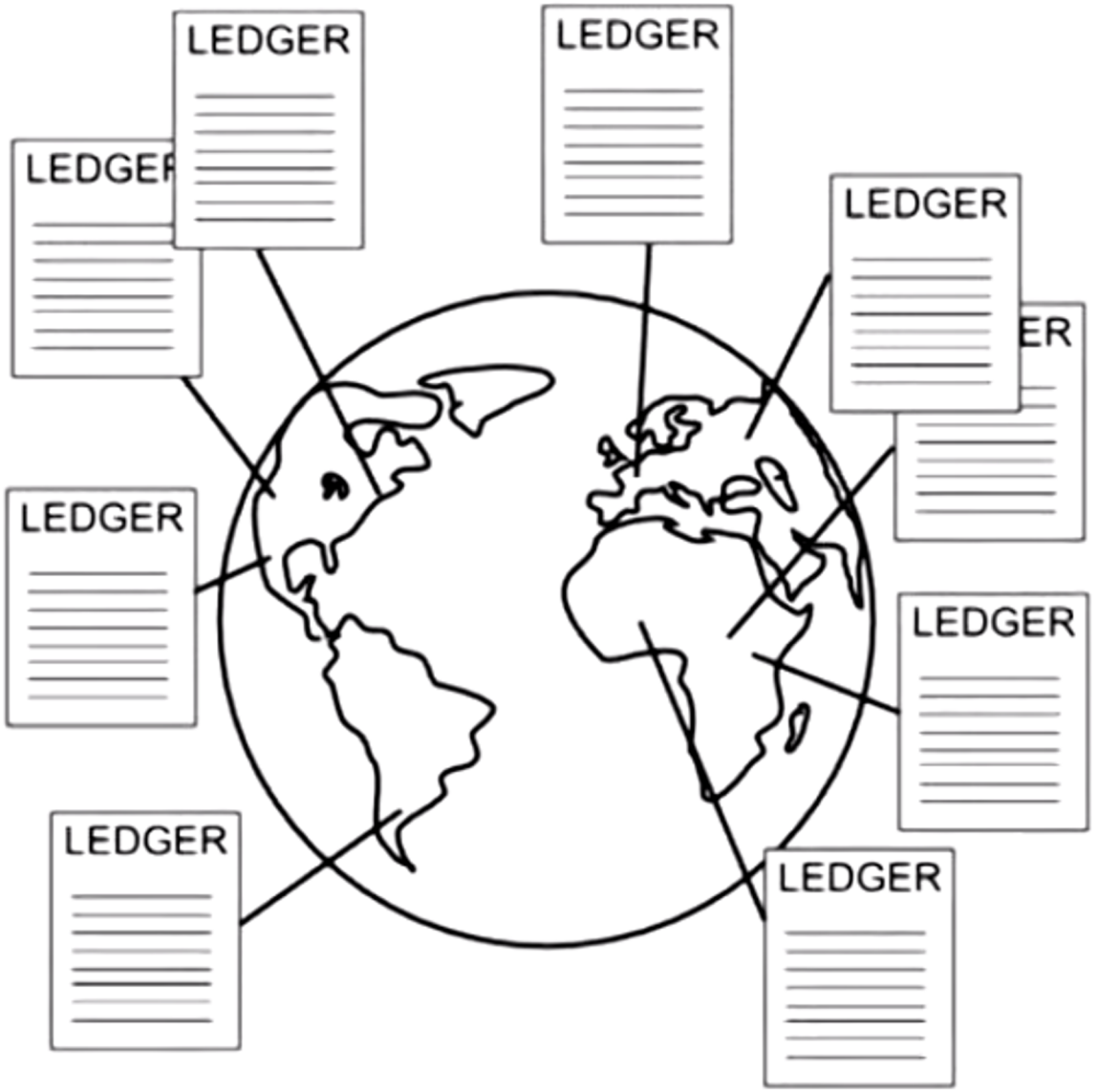
CHEQUING ACCOUNT STATEMENT
Page : 1 of 1

JOHN JONES
1643 DUNDAS ST W APT 27
TORONTO ON M6K 1V2

Statement period	Account No.
2003-10-09 to 2003-11-08	00005-123-456-7

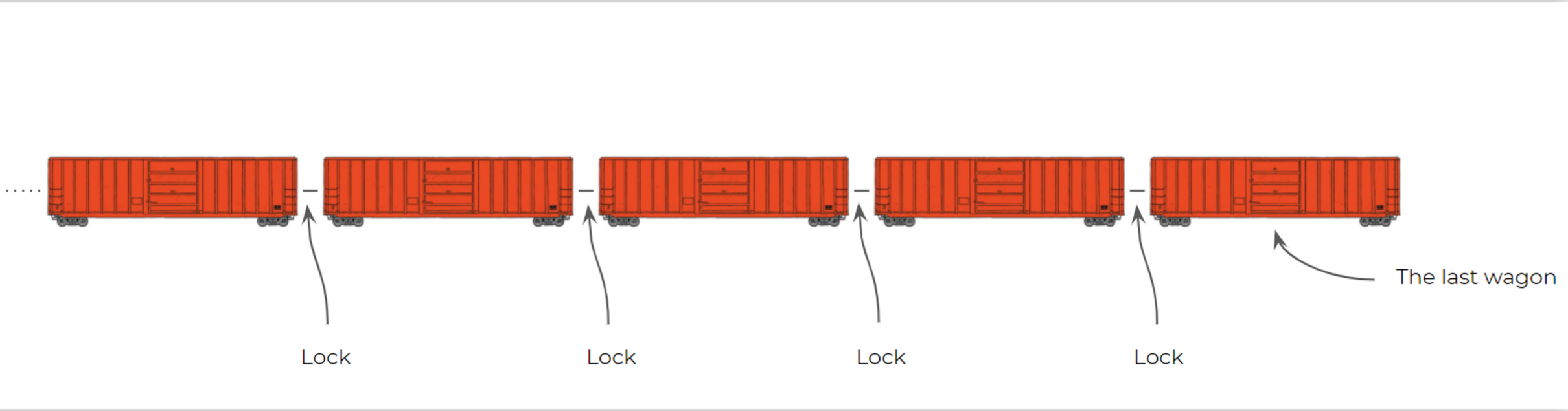
Date	Description	Ref.	Withdrawals	Deposits	Balance
2003-10-08	Previous balance				0.55
2003-10-14	Payroll Deposit - HOTEL			694.81	695.36
2003-10-14	Web Bill Payment - MASTERCARD	9685	200.00		495.36
2003-10-16	ATM Withdrawal - INTERAC	3990	21.25		474.11
2003-10-16	Fees - Interac		1.50		472.61
2003-10-20	Interac Purchase - ELECTRONICS	1975	2.99		469.62
2003-10-21	Web Bill Payment - AMEX	3314	300.00		169.62
2003-10-22	ATM Withdrawal - FIRST BANK	0064	100.00		69.62
2003-10-23	Interac Purchase - SUPERMARKET	1559	29.08		40.54
2003-10-24	Interac Refund - ELECTRONICS	1975		2.99	43.53
2003-10-27	Telephone Bill Payment - VISA	2475	6.77		36.76
2003-10-28	Payroll Deposit - HOTEL			694.81	731.57
2003-10-30	Web Funds Transfer - From SAVINGS	2620		50.00	781.57
2003-11-03	Pre-Auth. Payment - INSURANCE		33.55		748.02
2003-11-03	Cheque No. - 409		100.00		648.02
2003-11-06	Mortgage Payment		710.49		-62.47
2003-11-07	Fees - Overdraft		5.00		-67.47
2003-11-08	Fees - Monthly		5.00		-72.47
	*** Totals ***		1,515.63	1,442.61	

FUTURE OF PRIVACY FORUM



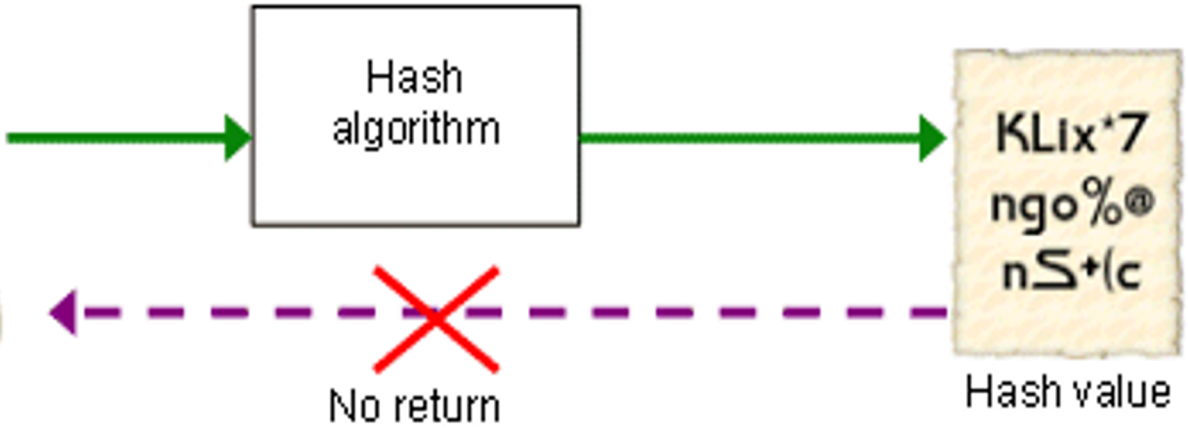
FUTURE OF PRIVACY FORUM

FUTURE OF PRIVACY FORUM



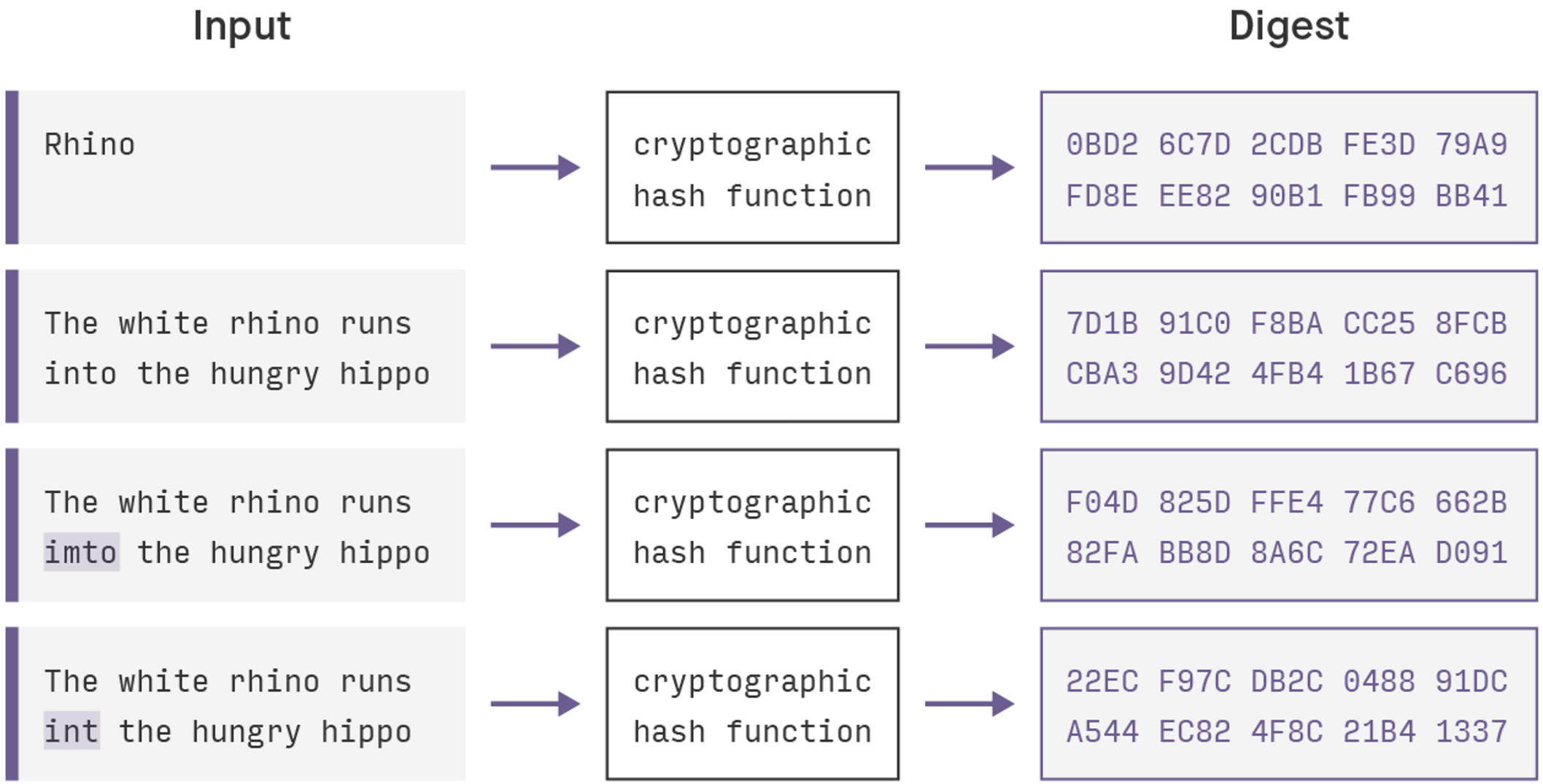
FUTURE OF PRIVACY FORUM

The cryptographic hash function

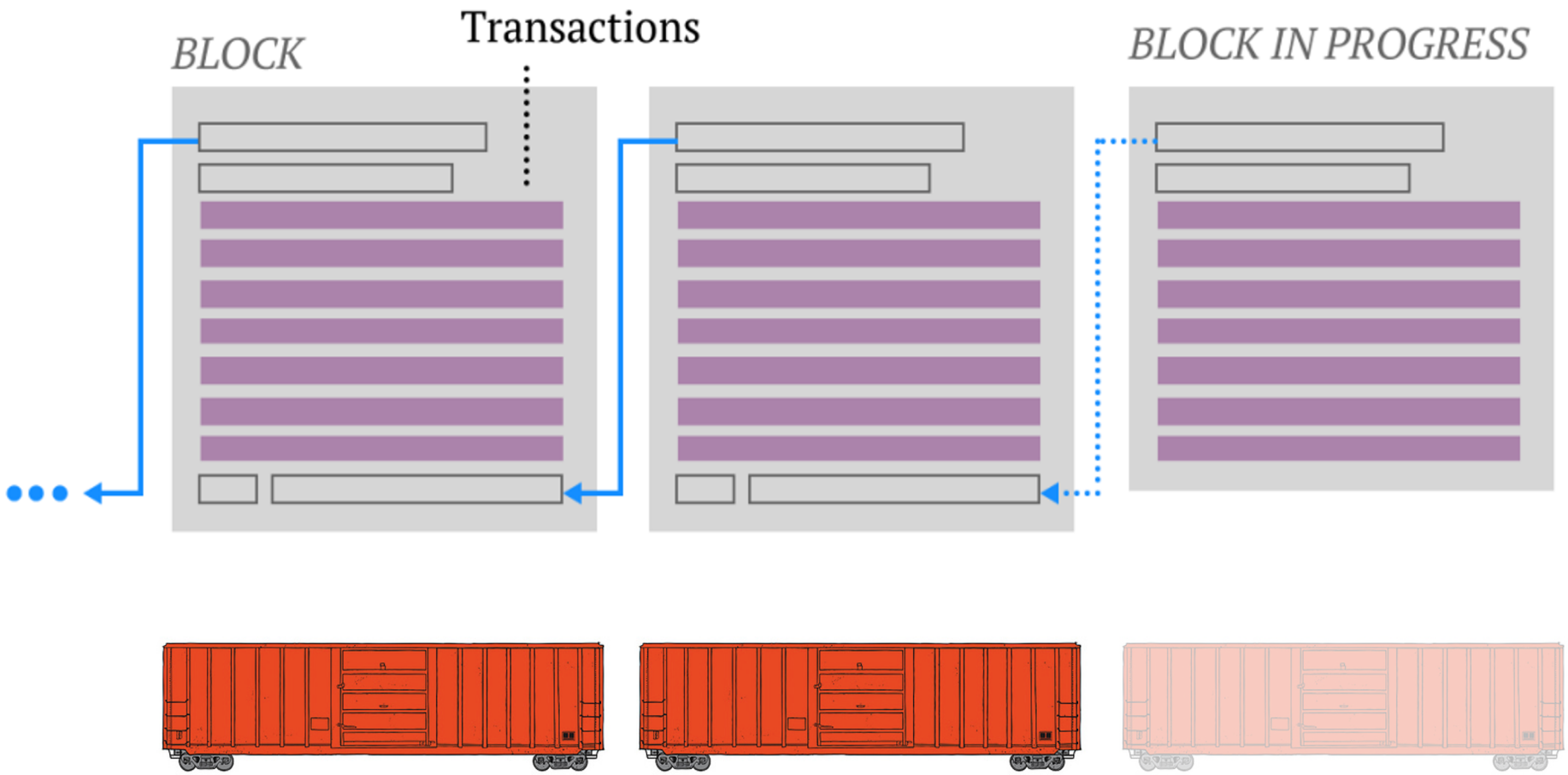


Unique for structured data

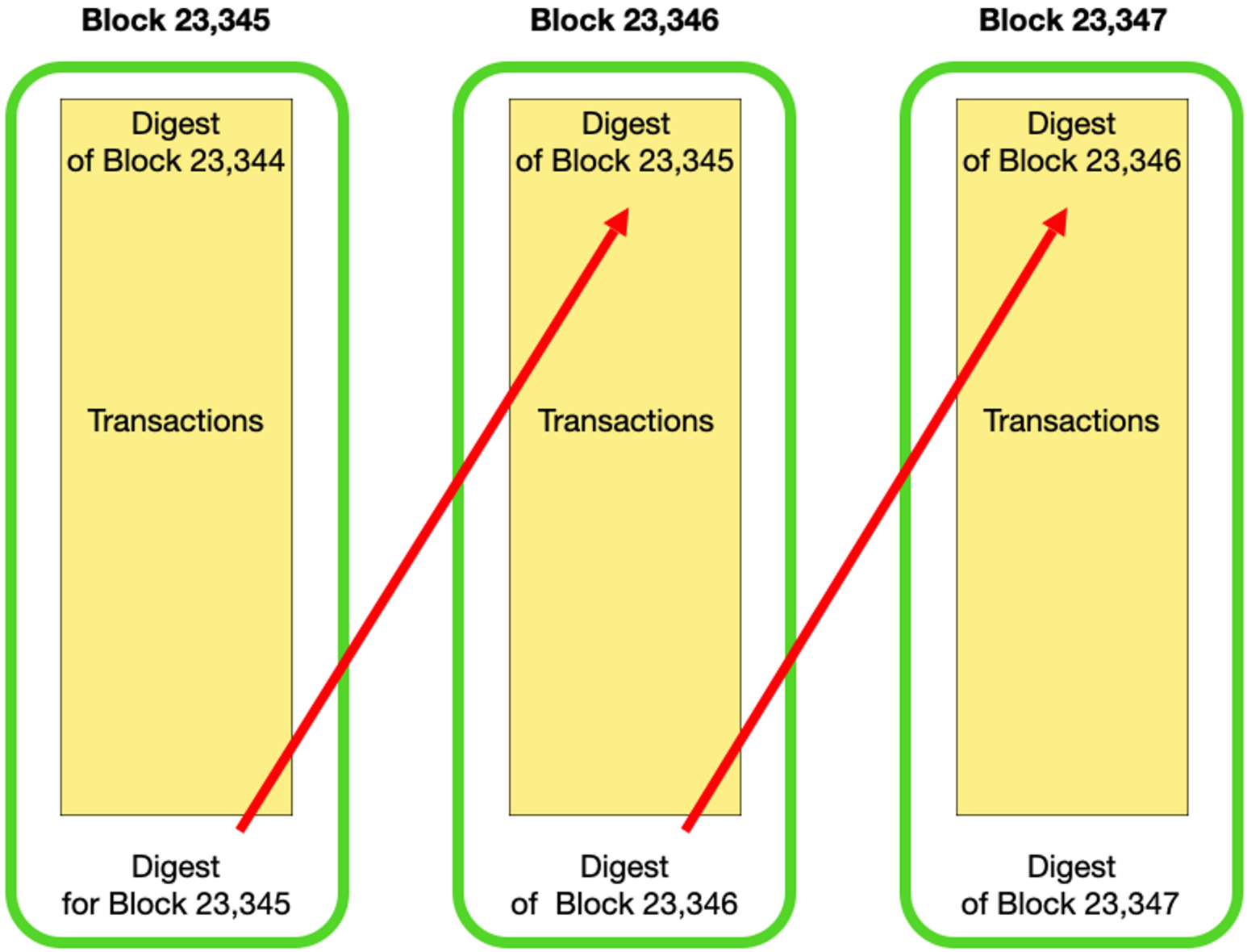
FUTURE OF PRIVACY FORUM



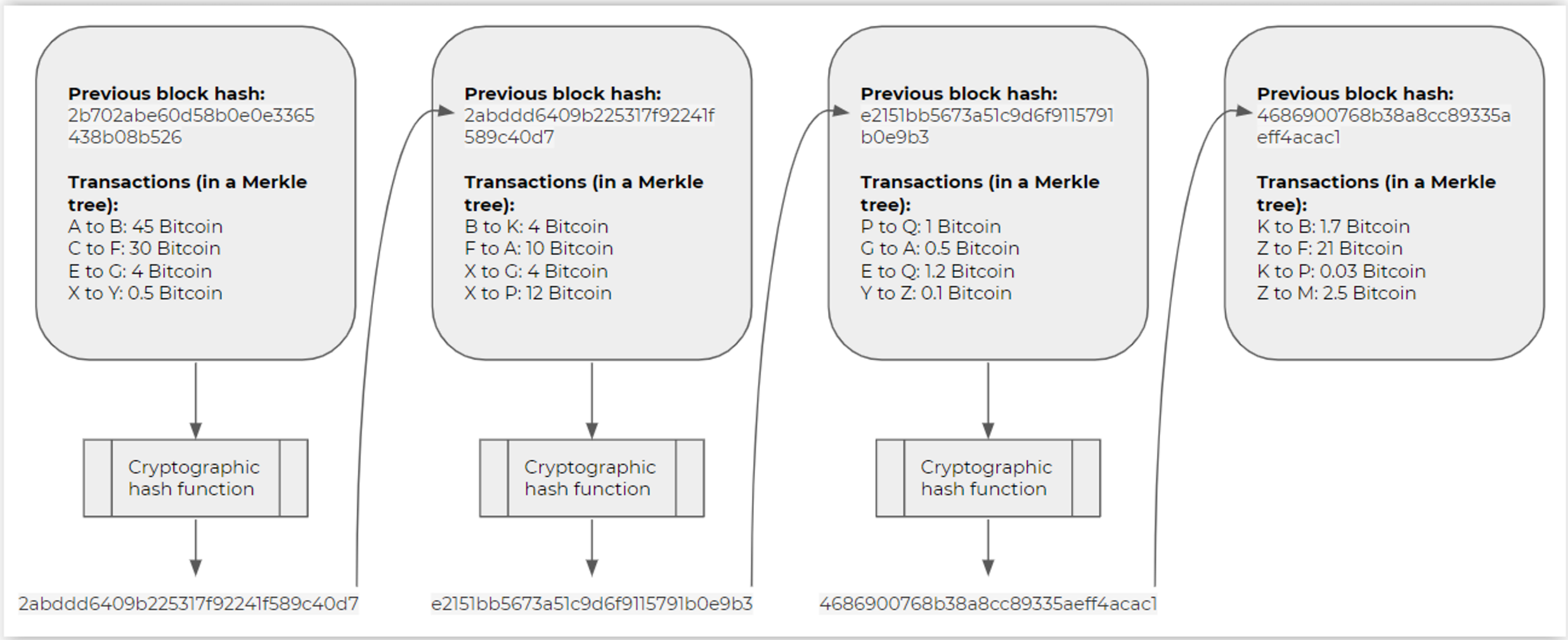
FUTURE OF PRIVACY FORUM



FUTURE OF PRIVACY FORUM

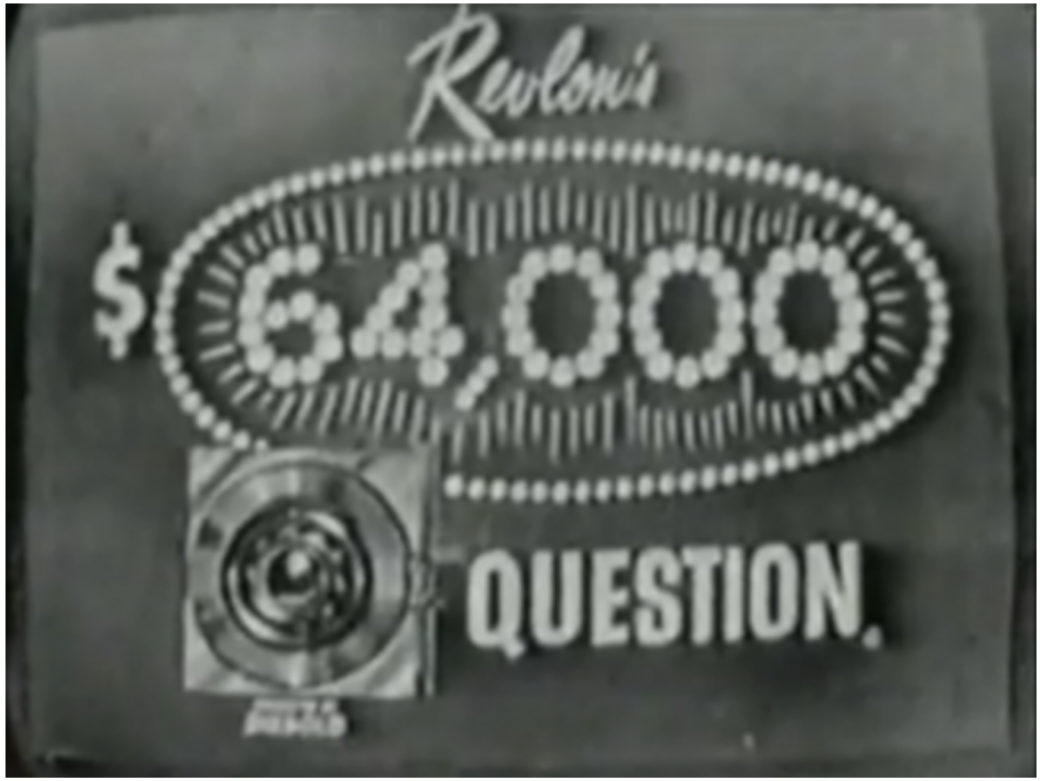


FUTURE OF PRIVACY FORUM



FUTURE OF PRIVACY FORUM

How to prevent “re-doing the whole train”?

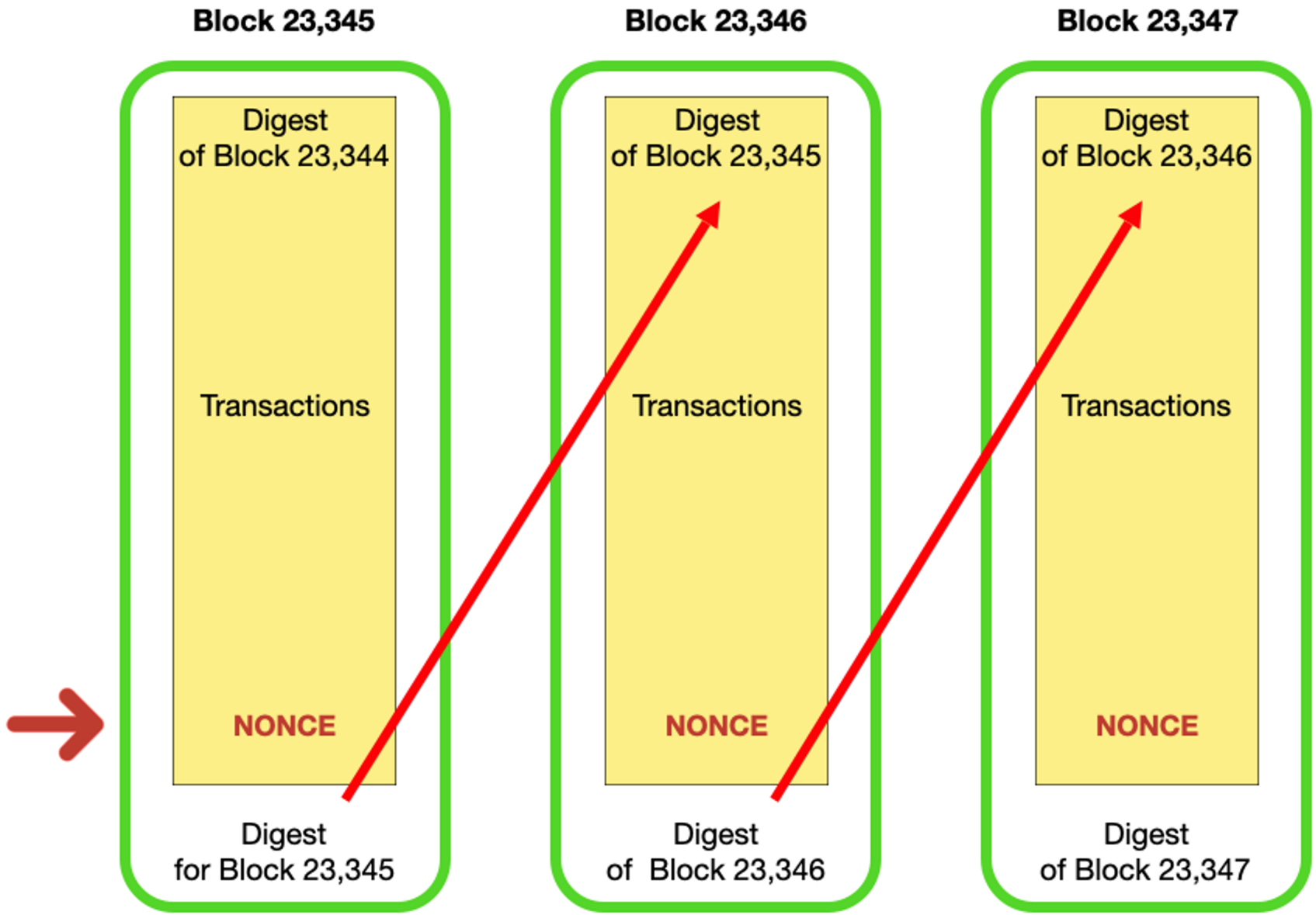


FUTURE OF PRIVACY FORUM

Adding “proof of work”

- Think of it as a ***time cost*** - in essence impose a 10 minute delay on the addition of a new block
- Make re-calculation, and thus change, (almost) impossible

The “**nonce**”



FUTURE OF PRIVACY FORUM

A sample SHA-256 hash digest:

`1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64`

(This is really nothing more than a number between 1 and 2^256 in hexadecimal format)

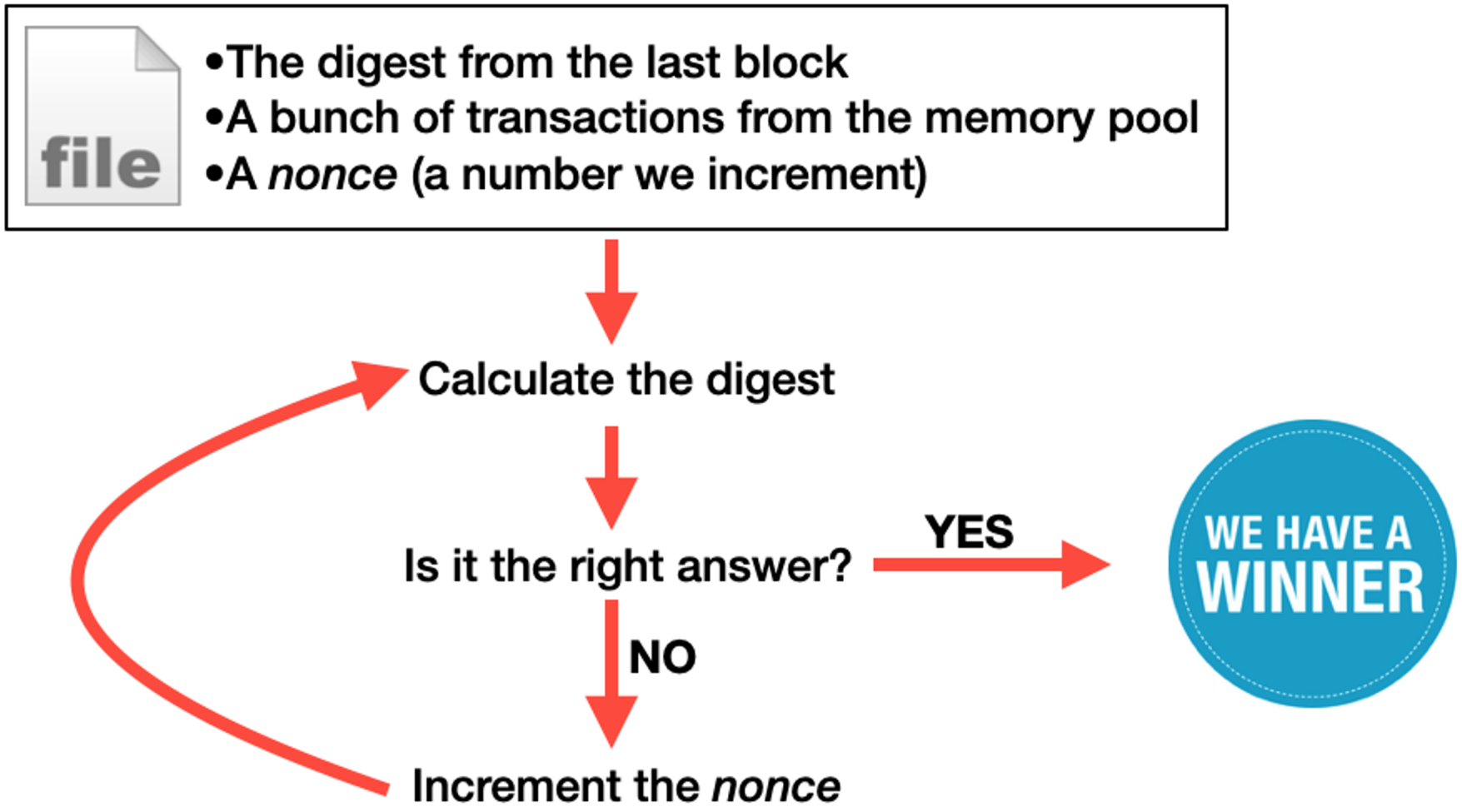
FUTURE OF PRIVACY FORUM

The type of hash we are looking for:

0000000000000000b42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8

FUTURE OF PRIVACY FORUM

Retrying with a different nonce: "mining"



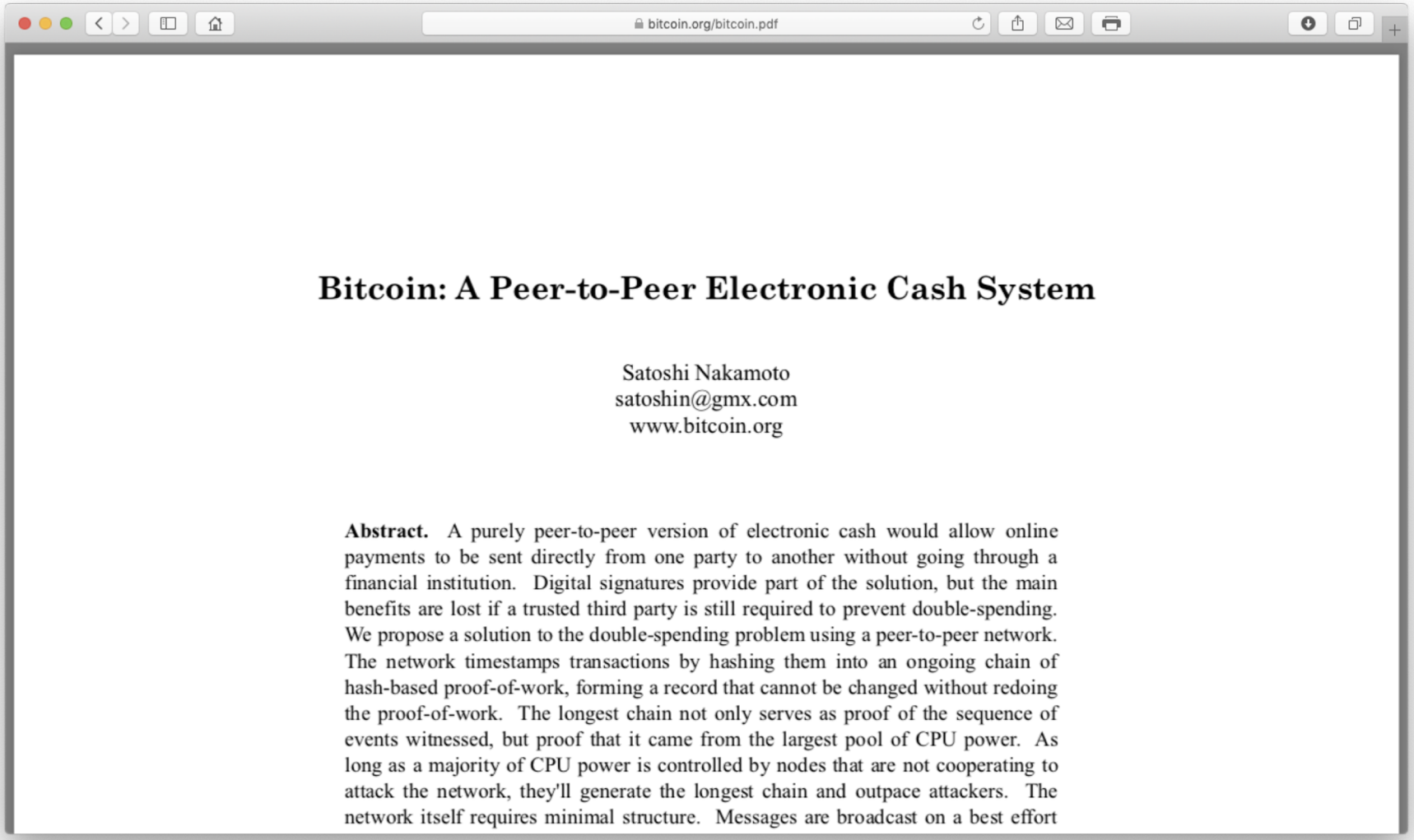
FUTURE OF PRIVACY FORUM

When a winner is found

1. The winning node messages all other nodes: I found a winner!
2. Other nodes verify the hash and if OK accept the new block
3. Once 51% of all nodes have accepted the block, it is “confirmed”
4. The winning node gets a reward (currently 6.75 bitcoin)
5. Start all over again!

FUTURE OF PRIVACY FORUM

Use case: cryptocurrencies



FUTURE OF PRIVACY FORUM

From: Satoshi Nakamoto <satoshi <at> vistomail.com>
Subject: Bitcoin P2P e-cash paper
Newsgroups: gmane.comp.encryption.general
Date: 2008-10-31 18:10:00 GMT

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.
The paper is available at: http://www.bitcoin.org/bitcoin.pdf
The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System
Abstract. A purely peer-to-peer version of electronic cash [...]

Satoshi Nakamoto

The Cryptography Mailing List

FUTURE OF PRIVACY FORUM

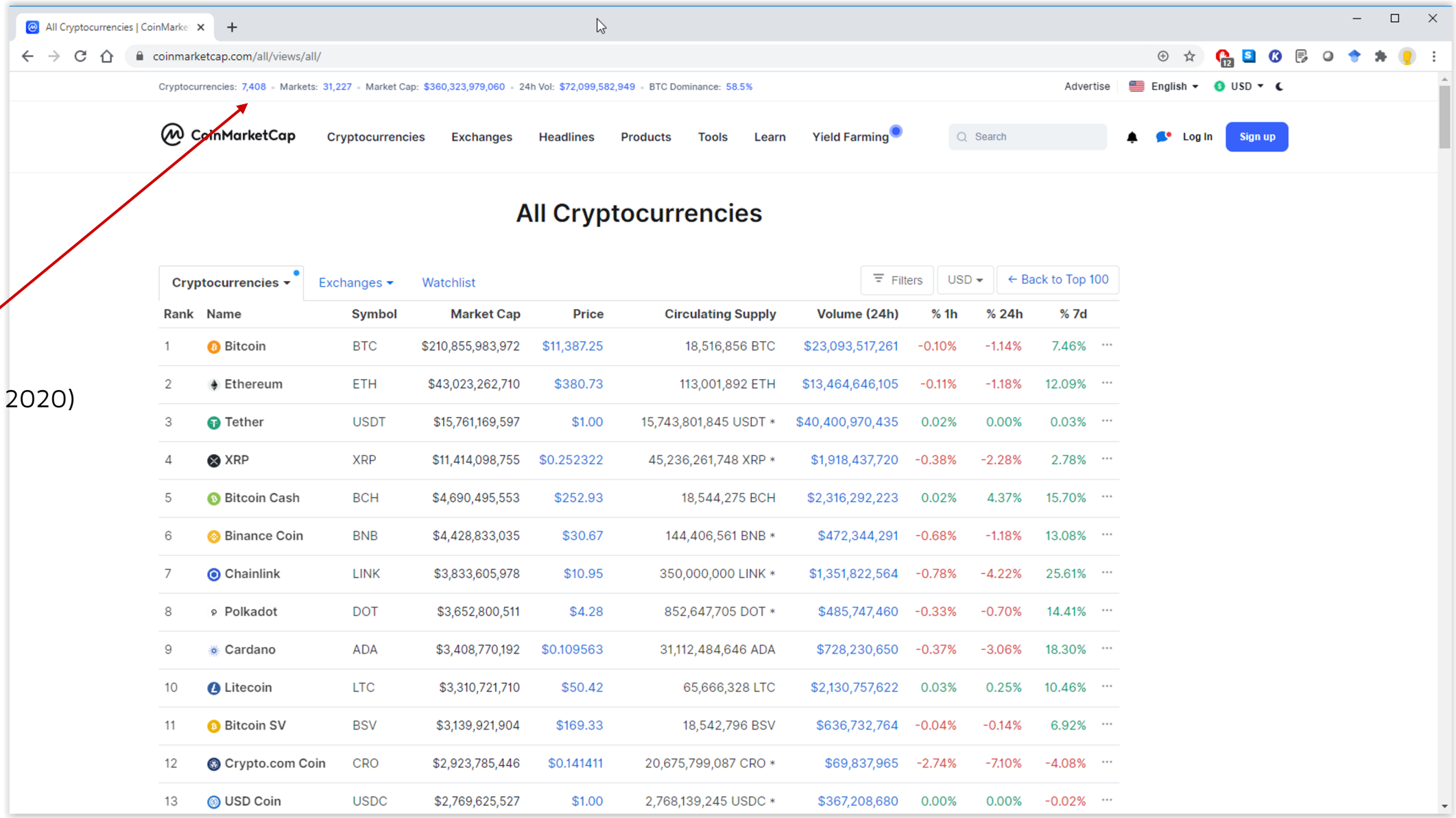
- Transactions are authorized by the owner's **private** key (can be stored in a *digital wallet*)

- Ownership on the blockchain is tracked by the owner's **public** key address, e.g.:

0x9A134Ce4BBd8c7b3A262774Fafd60B7f7ce3655B

FUTURE OF PRIVACY FORUM

7,408 (as of 14 oct 2020)



Rank	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$210,855,983,972	$11,387.25	18,516,856 BTC	$23,093,517,261	-0.10%	-1.14%	7.46%
2	Ethereum	ETH	$43,023,262,710	$380.73	113,001,892 ETH	$13,464,646,105	-0.11%	-1.18%	12.09%
3	Tether	USDT	$15,761,169,597	$1.00	15,743,801,845 USDT *	$40,400,970,435	0.02%	0.00%	0.03%
4	XRP	XRP	$11,414,098,755	$0.252322	45,236,261,748 XRP *	$1,918,437,720	-0.38%	-2.28%	2.78%
5	Bitcoin Cash	BCH	$4,690,495,553	$252.93	18,544,275 BCH	$2,316,292,223	0.02%	4.37%	15.70%
6	Binance Coin	BNB	$4,428,833,035	$30.67	144,406,561 BNB *	$472,344,291	-0.68%	-1.18%	13.08%
7	Chainlink	LINK	$3,833,605,978	$10.95	350,000,000 LINK *	$1,351,822,564	-0.78%	-4.22%	25.61%
8	Polkadot	DOT	$3,652,800,511	$4.28	852,647,705 DOT *	$485,747,460	-0.33%	-0.70%	14.41%
9	Cardano	ADA	$3,408,770,192	$0.109563	31,112,484,646 ADA	$728,230,650	-0.37%	-3.06%	18.30%
10	Litecoin	LTC	$3,310,721,710	$50.42	65,666,328 LTC	$2,130,757,622	0.03%	0.25%	10.46%
11	Bitcoin SV	BSV	$3,139,921,904	$169.33	18,542,796 BSV	$636,732,764	-0.04%	-0.14%	6.92%
12	Crypto.com Coin	CRO	$2,923,785,446	$0.141411	20,675,799,087 CRO *	$69,837,965	-2.74%	-7.10%	-4.08%
13	USD Coin	USDC	$2,769,625,527	$1.00	2,768,139,245 USDC *	$367,208,680	0.00%	0.00%	-0.02%

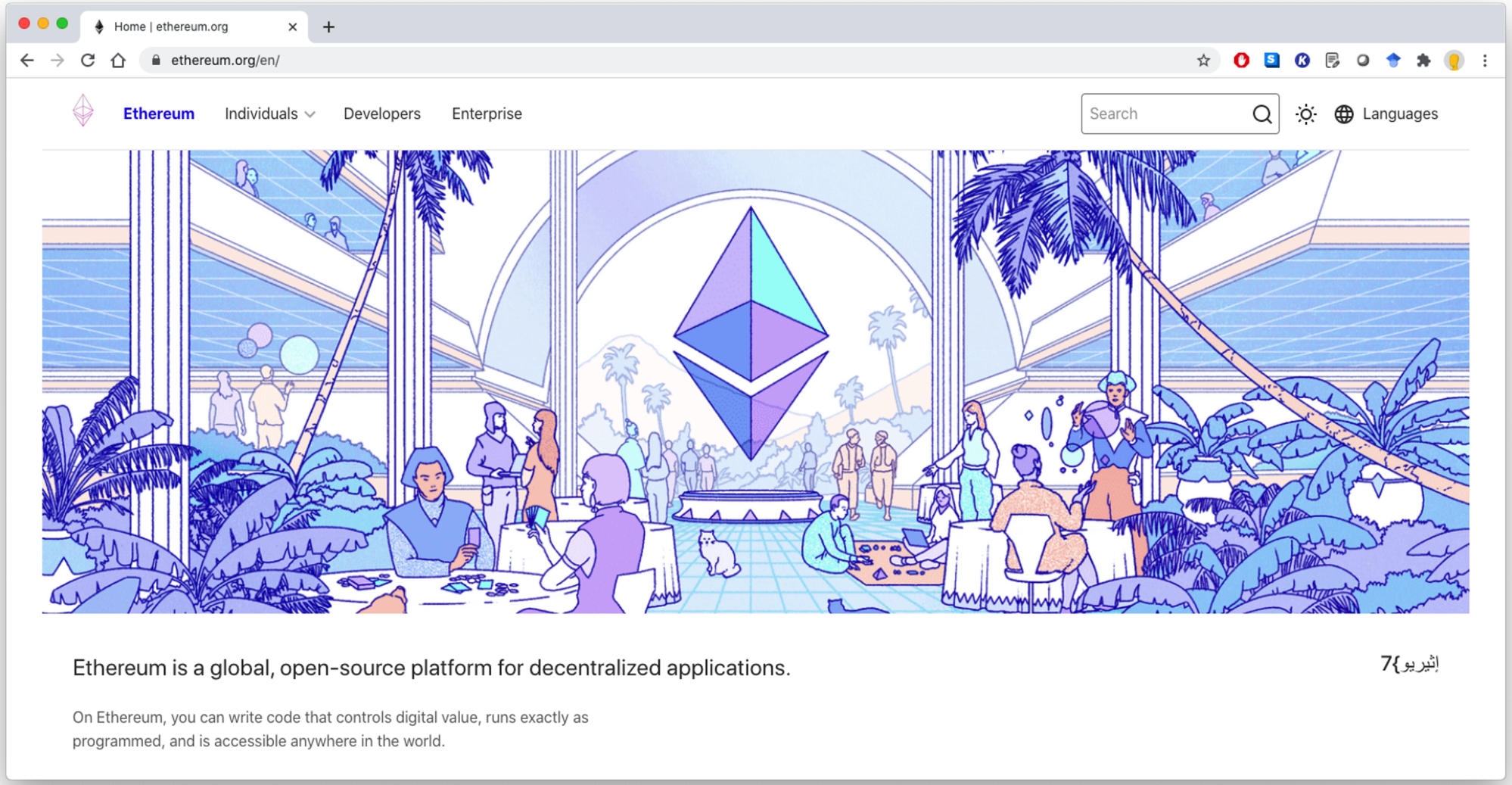
FUTURE OF PRIVACY FORUM

How blockchain implementations differ

- How new transactions are confirmed and added (consensus mechanisms):
  - Proof of Stake (e.g. Peercoin)
  - Byzantine Fault Tolerance (vote based) approaches (e.g. Ripple)
  - Directed Acyclic Graphs (e.g. Iota)
  - Proof of Elapsed Time
  - etc.

- Who can use the blockchain:
  - public (permissionless) blockchains
  - private (permissioned) blockchains

Blockchain as a platform



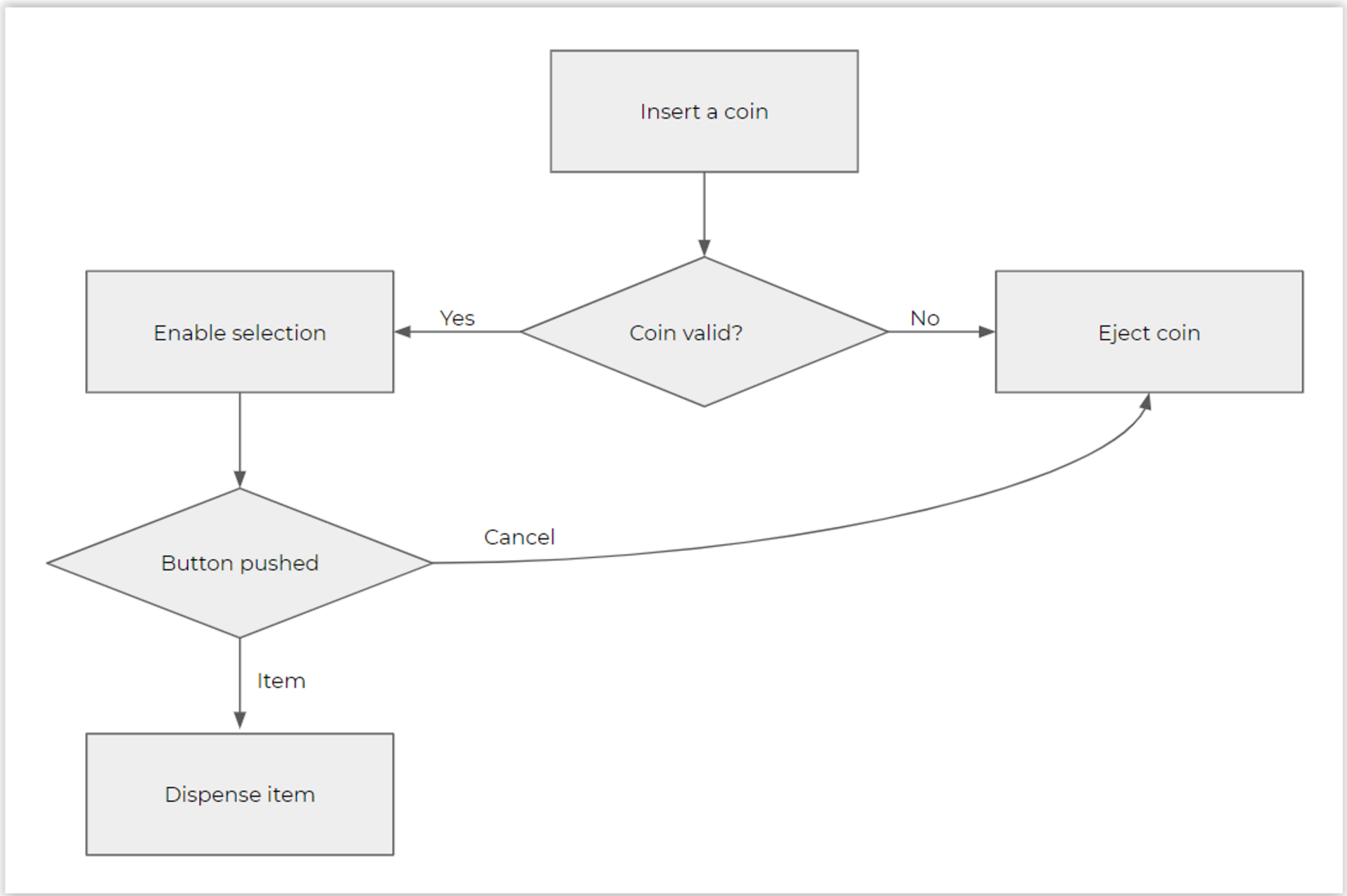
FUTURE OF PRIVACY FORUM

Features

- Tracks transactions
- Is also able to store small bits of computer code ("smart contracts")
- Code runs within the Ethereum platform and changes the **state** of **variables** (think entitlements) stored on the blockchain
- Uses the ***ether*** cryptocurrency
- Also uses ***gas*** to pay for running the computer code
- Has a much shorter confirmation time (about 15 seconds)
- "DApps" are built on top of these platforms

“Smart” contracts

FUTURE OF PRIVACY FORUM



FUTURE OF PRIVACY FORUM

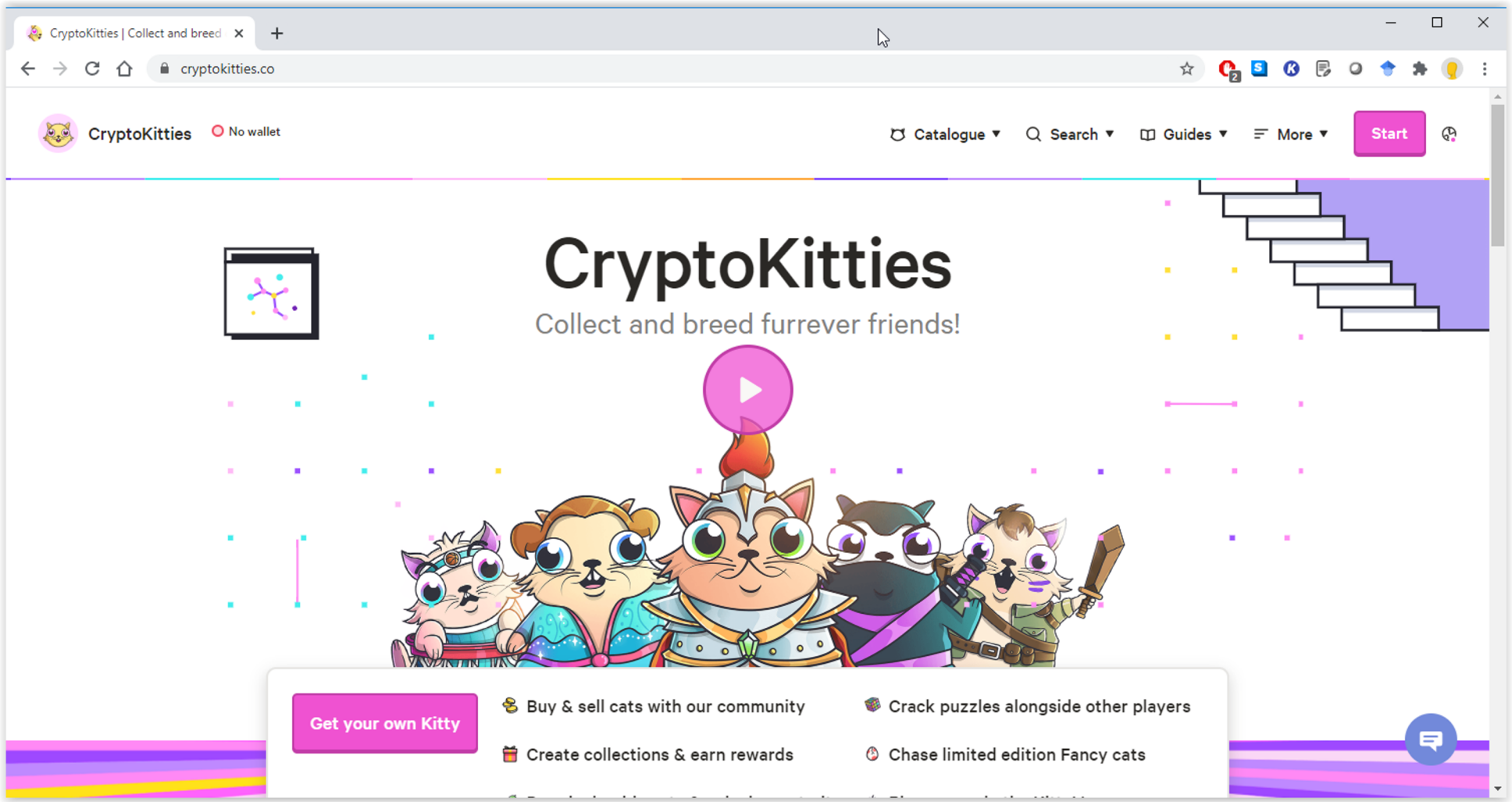
Use case: Tokens

FUTURE OF PRIVACY FORUM

```
pragma solidity ^0.4.16;

contract MyToken {
    // This creates an array with all balances
    mapping (address => uint256) public balanceOf;

    // Initializes contract with initial supply tokens to the creator of the contract
    function MyToken(
        uint256 initialSupply
    ) {
        balanceOf[msg.sender] = initialSupply;              // Give the creator all initial tokens
    }

    // Send coins
    function transfer(address _to, uint256 _value) {
        require(balanceOf[msg.sender] >= _value);           // Check if the sender has enough
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows
        balanceOf[msg.sender] -= _value;                    // Subtract from the sender
        balanceOf[_to] += _value;                           // Add the same to the recipient
    }
}
```

FUTURE OF PRIVACY FORUM

Use case: CryptoKitties



FUTURE OF PRIVACY FORUM

End of the technical intro

FUTURE OF PRIVACY FORUM