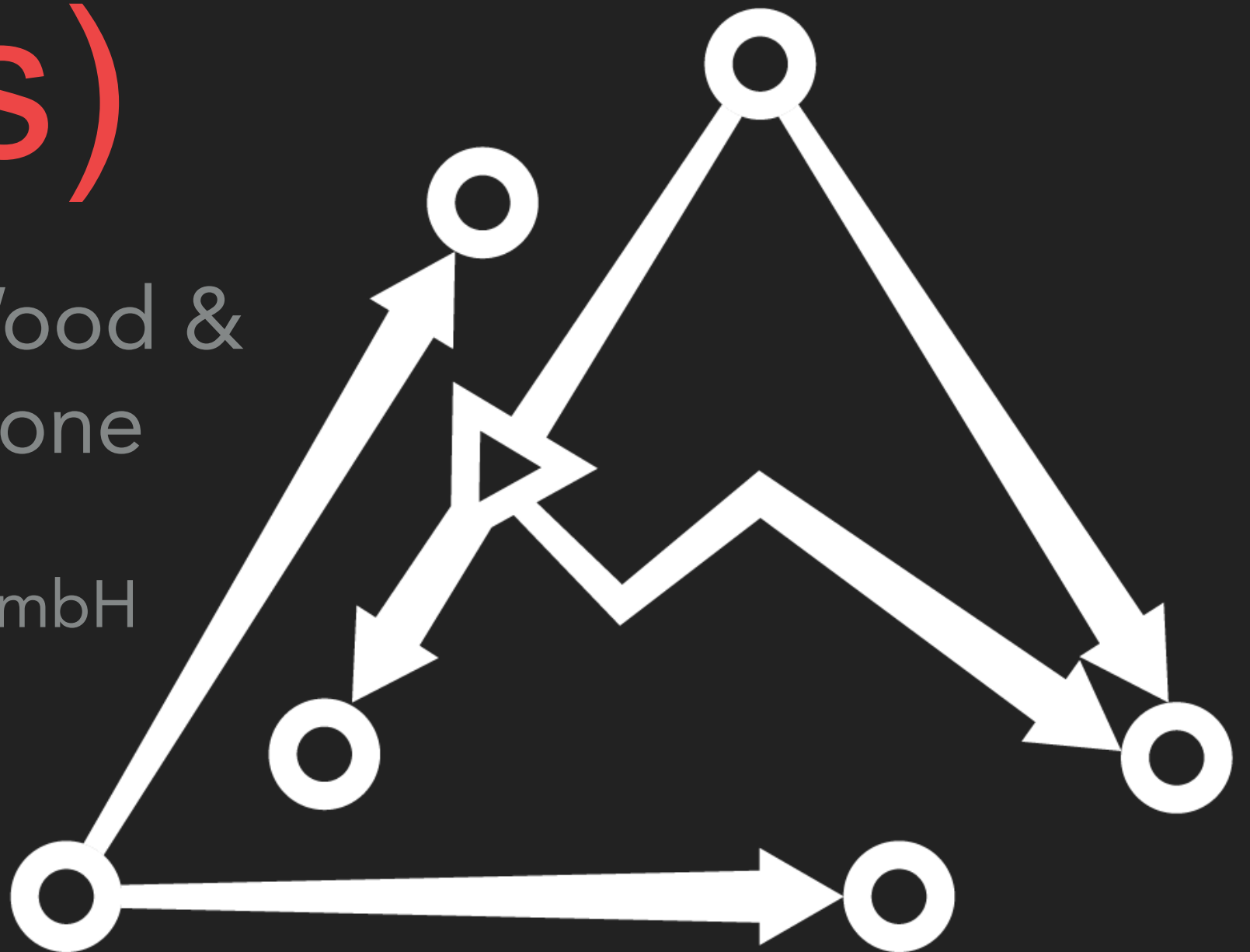


Zero-Knowledge Access Passes (ZKAPs)

Christopher R. Wood &
Jean-Paul Calderone

Least Authority TFA GmbH

Zeal Call - March 31, 2020





FOCUS ON SECURITY

We help projects improve their security and build secure technology.

From prototype to production, we work closely with teams through the complete development cycle to identify security issues and promote best practices. Our consulting services include security audits, design reviews and multi-phase engagements.

[Learn More](#)[Schedule a Call](#)

PUBLISHED AUDIT REPORTS



ZCash

Three Audits



Ethereum

Incentive Analysis



Blockstack

Stacks Investor Wallet



MetaMask

Mobile App



Tezos

Five Audits

PRIVACY BY DESIGN

At Least Authority, we believe in peoples' right to privacy and are on a mission to make secure technology easy and accessible to everyone. We build technical solutions that incorporate these values and help technologies to be more secure.

[Co-Founded Ventures](#)[Open Source Projects](#)

[ECC Posts](#) / [Spinning Off Our Sibling Company](#)

Spinning Off Our Sibling Company

Zooko Wilcox | March 20, 2017

The Zcash company grew out of a company named "Least Authority". It was when we were Least Authority that we did a security audit of Ethereum and several other successful security audits ([CryptoCat](#), [GlobalLeaks](#), [SpiderOak](#), and [Ooni](#)). Least Authority also developed the advanced cryptographically-protected, decentralized file store, [Tahoe-LAFS](#).

When we formed a new company to launch Zcash (the "ZeroCoin Electric Coin Company", a.k.a. "The Zcash Company"), we split off from Least Authority and at first I tried to continue acting as the CEO of both companies at once. Perhaps I was influenced by the legends of Elon Musk and Jack Dorsey, two people who currently serve as CEOs of two different companies.

But you know what? No way was that going to work. The run-up to the Zcash launch consumed all of my time and attention, and the Least Authoritarians continued to develop their cutting-edge open source technology, but they had to do so without any business support from me.

Therefore I'm delighted to announce that our sibling company, Least Authority, now has a new full-time CEO: Liz Steininger. I've worked with Liz before on Internet freedom technology; I trust her ethics and her judgment. Her excellent skills at organization, planning, and business are a good match for the excellent cryptography and coding skills of the other Least Authoritarians.

Least Authority has incorporated in Berlin, Germany (the world capitol for Internet freedom hackers) and launched a new web site. The team continues to do specialized security audits and create freedom-compatible technologies, and has some big things in the works that you'll hear more about soon, including a user-friendly way to use their secure storage product.

Right now you can sign up for Least Authority's "S4" service, which is a cloud storage service built on top of Amazon S3, with the addition of our advanced open source end-to-end encryption so that your data is never exposed to snooping or injection.

(P.S. For fans of cryptocurrency history, here's that time I posted about Tahoe-LAFS on BitcoinTalk.org back in 2010 and [Satoshi Nakamoto replied](#).)

What are ZKAPs?

- ▶ ZKAPs = Zero-Knowledge Access Passes
- ▶ An anonymous, token-based authorization protocol

What are ZKAPs?

- ▶ ZKAPs = Zero-Knowledge Access Passes
- ▶ An anonymous, token-based authorization protocol
- ▶ See also: Privacy Pass <<https://privacypass.github.io>>

What are ZKAPs?

- ▶ ZKAPs = Zero-Knowledge Access Passes
- ▶ An anonymous, token-based authorization protocol
- ▶ See also: Privacy Pass <<https://privacypass.github.io>>
- ▶ (To be) used by PrivateStorage <<https://privatestorage.io>>

PrivateStorage has been designed with privacy and security features to give you the control of who has access to your data. We cannot see your data when it is stored by us

FEATURES



Client-side Encryption

All files are encrypted before leaving your local device, preserving the confidentiality and integrity of your data.



Accountless Authorization

Files stored are accessed through the use of special codes known as capabilities, not using passwords or email addresses, for enhanced security and privacy.



Bi-directional Folder Synchronization

Regularly and automatically sync your local files with the cloud and your other devices.



Multiple Device Support

Share access to specific folders across multiple devices that you own.



Native Desktop Integration

Easy-to-use, simple desktop applications for all major desktop operating systems: macOS, Linux and Windows.



No Data or Vendor Lock-in

Retain control over your data with an open protocol design and complete software transparency with open source code.

PrivateStorage has been designed with privacy and security features to give you the control of who has access to your data. We cannot see your data when it is stored by us

FEATURES



Client-side Encryption

All files are encrypted before leaving your local device, preserving the confidentiality and integrity of your data.



Accountless Authorization

Files stored are accessed through the use of special codes known as capabilities, not using passwords or email addresses, for enhanced security and privacy.



Bi-directional Folder Synchronization

Regularly and automatically sync your local files with the cloud and your other devices.



Multiple Device Support

Share access to specific folders across multiple devices that you own.



Native Desktop Integration

Easy-to-use, simple desktop applications for all major desktop operating systems: macOS, Linux and Windows.



No Data or Vendor Lock-in

Retain control over your data with an open protocol design and complete software transparency with open source code.

Why ZKAPs?

- ▶ Privacy problems with existing access-control (authentication) systems

Why ZKAPs?

- ▶ Privacy problems with existing access-control (authentication) systems
- ▶ Example: online/web accounts


Email


Enter password

Age

Continue

OR

 **Continue with Facebook**

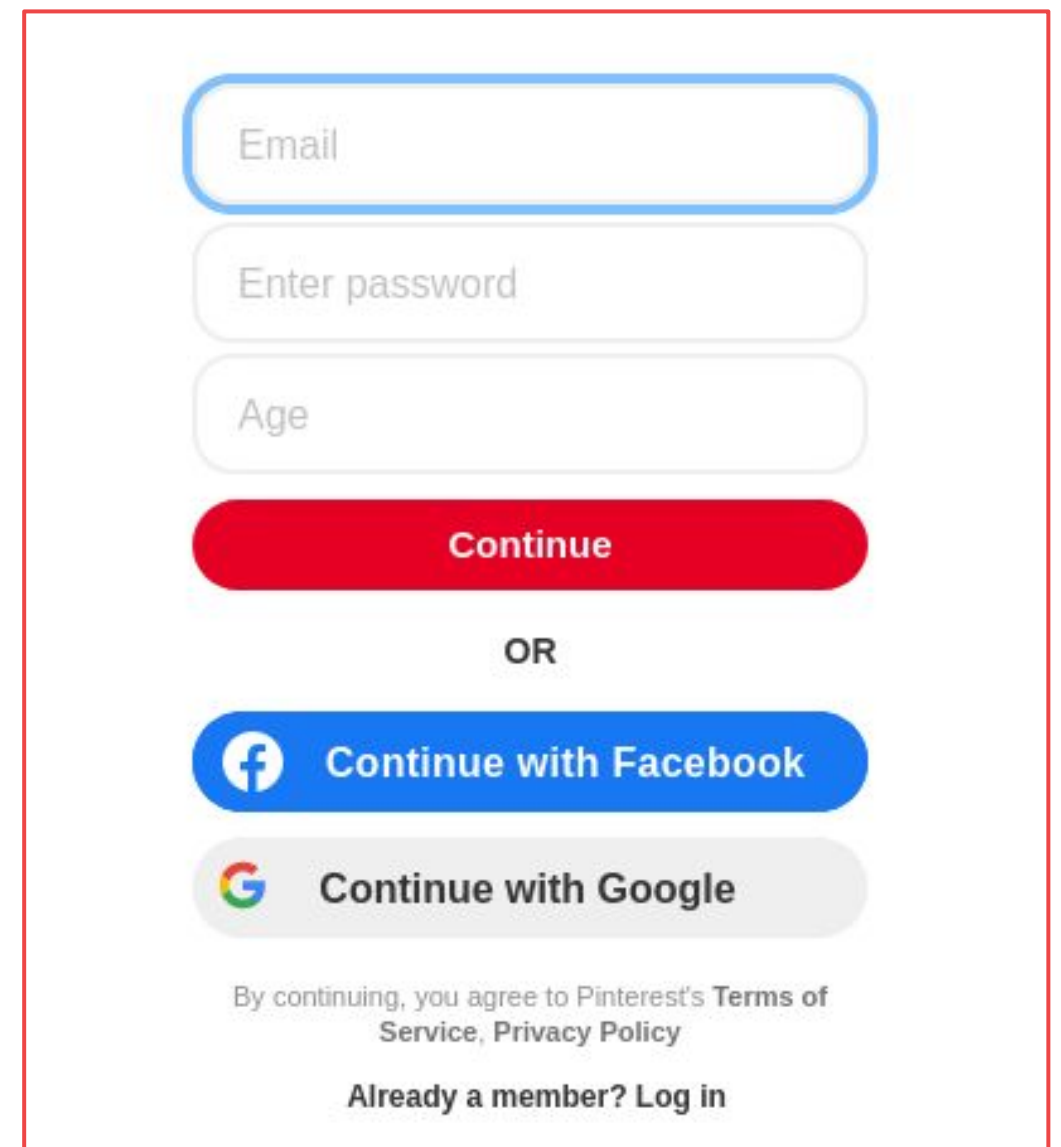
 **Continue with Google**

By continuing, you agree to Pinterest's [Terms of Service](#), [Privacy Policy](#)

Already a member? Log in

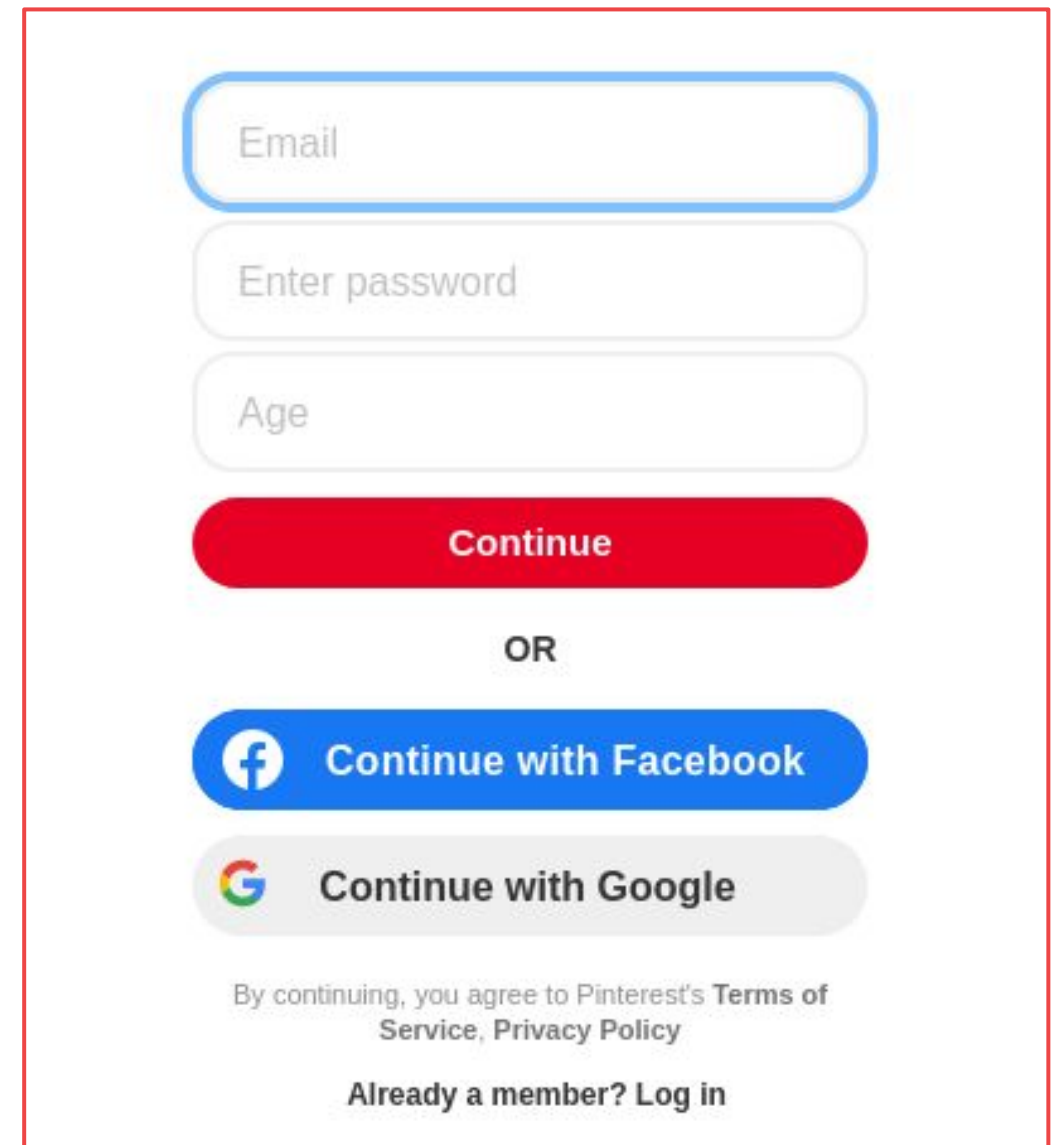
Why ZKAPs?

- ▶ Privacy problems with existing access-control (authentication) systems
- ▶ Example: online/web accounts
 - Durable identifiers (username, email, etc.) to *authenticate* users
 - Used to prevent abuse, free-riding, etc.

A screenshot of a login form for Pinterest, enclosed in a red rectangular border. The form contains three input fields: 'Email', 'Enter password', and 'Age'. Below these is a red 'Continue' button. Underneath the button is the word 'OR'. Following this are two social login options: 'Continue with Facebook' (with a blue button and Facebook icon) and 'Continue with Google' (with a grey button and Google icon). At the bottom, there is a line of small text: 'By continuing, you agree to Pinterest's Terms of Service, Privacy Policy' and a link 'Already a member? Log in'.

Why ZKAPs?

- ▶ Privacy problems with existing access-control (authentication) systems
- ▶ Example: online/web accounts
 - Durable identifiers (username, email, etc.) to *authenticate* users
 - Used to prevent abuse, free-riding, etc.
 - *But:*
 - Activity is linked to account
 - Accounts can be linked to individual account-holder(s)
 - Accounts can be compromised, etc.

A screenshot of a login form for Pinterest. It features three input fields: 'Email', 'Enter password', and 'Age'. Below these is a red 'Continue' button. A red box highlights the entire form area. Below the button is the word 'OR'. Then there are two social login buttons: 'Continue with Facebook' (blue with Facebook logo) and 'Continue with Google' (grey with Google logo). At the bottom, there is a link to 'Terms of Service, Privacy Policy' and a link for 'Already a member? Log in'.

Why ZKAPs?

- ▶ Privacy problems with existing access-control (authorization) systems

Why ZKAPs?

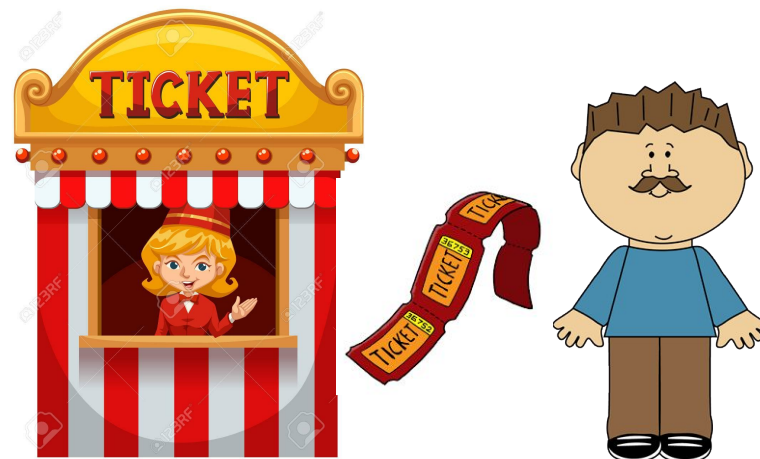
- ▶ Privacy problems with existing access-control (authorization) systems
- ▶ Example: ticket rolls:

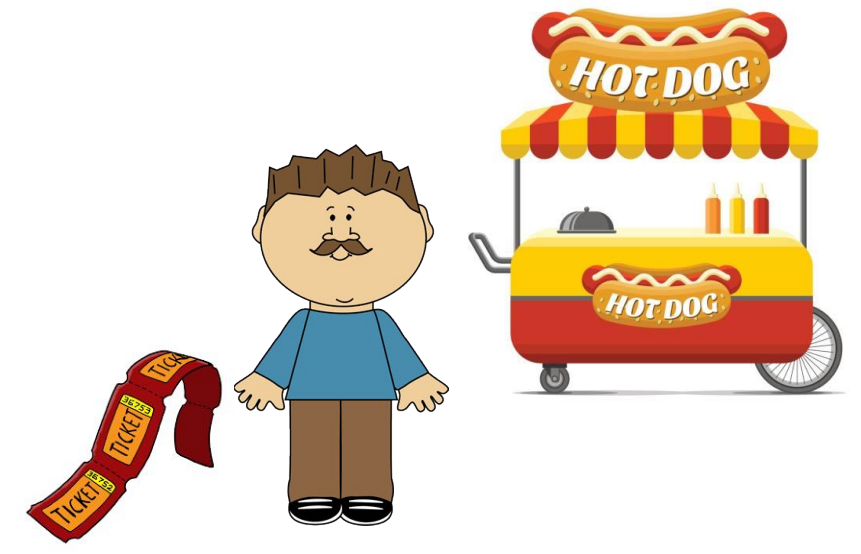
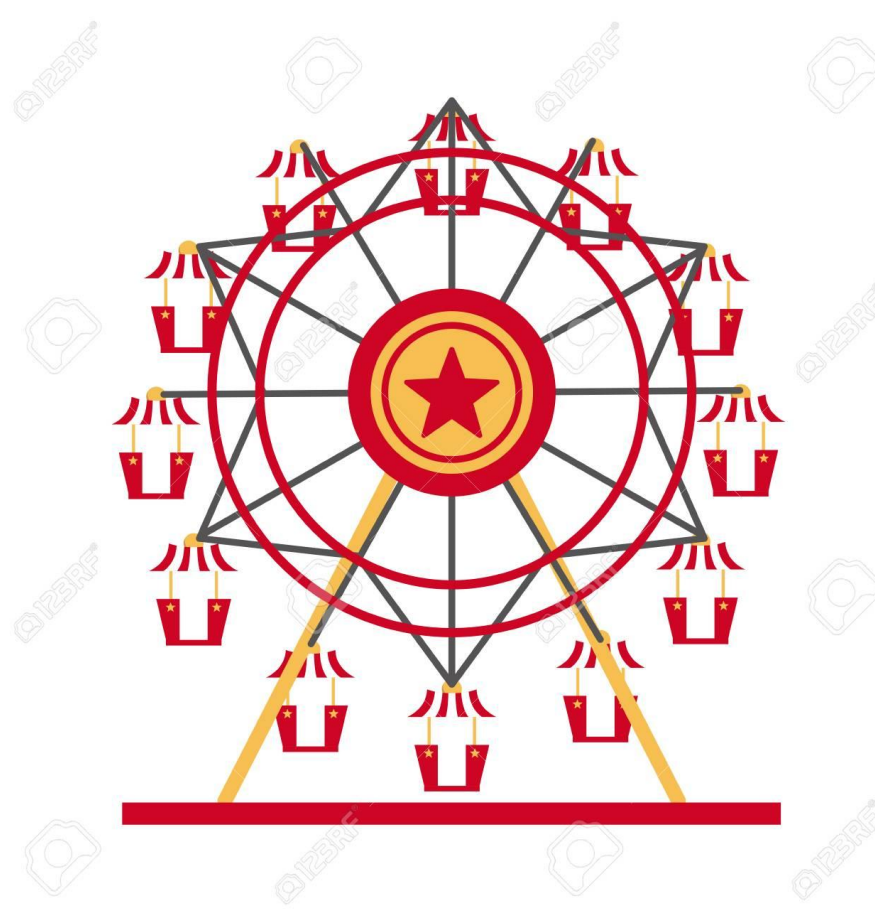


Why ZKAPs?

- ▶ Privacy problems with existing access-control (authorization) systems
- ▶ Example: ticket rolls:
 - Numbered labels to *authorize* ticket-holders
 - Corresponding “coupons” to *verify* disputes
 - Weakly “fungible”

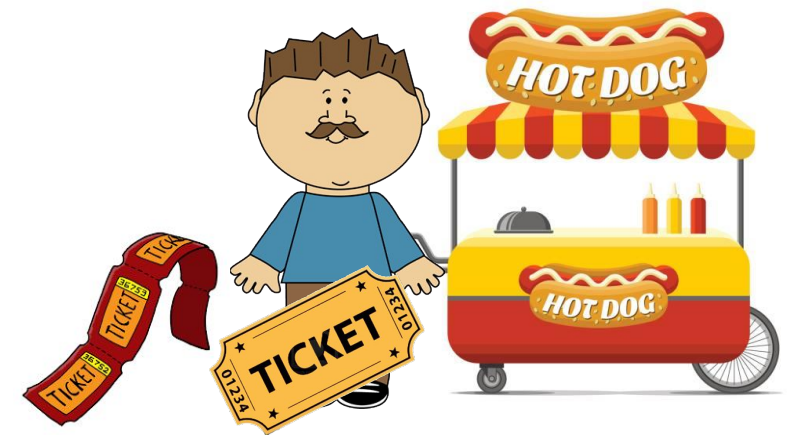






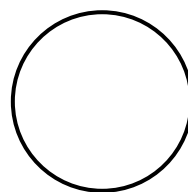
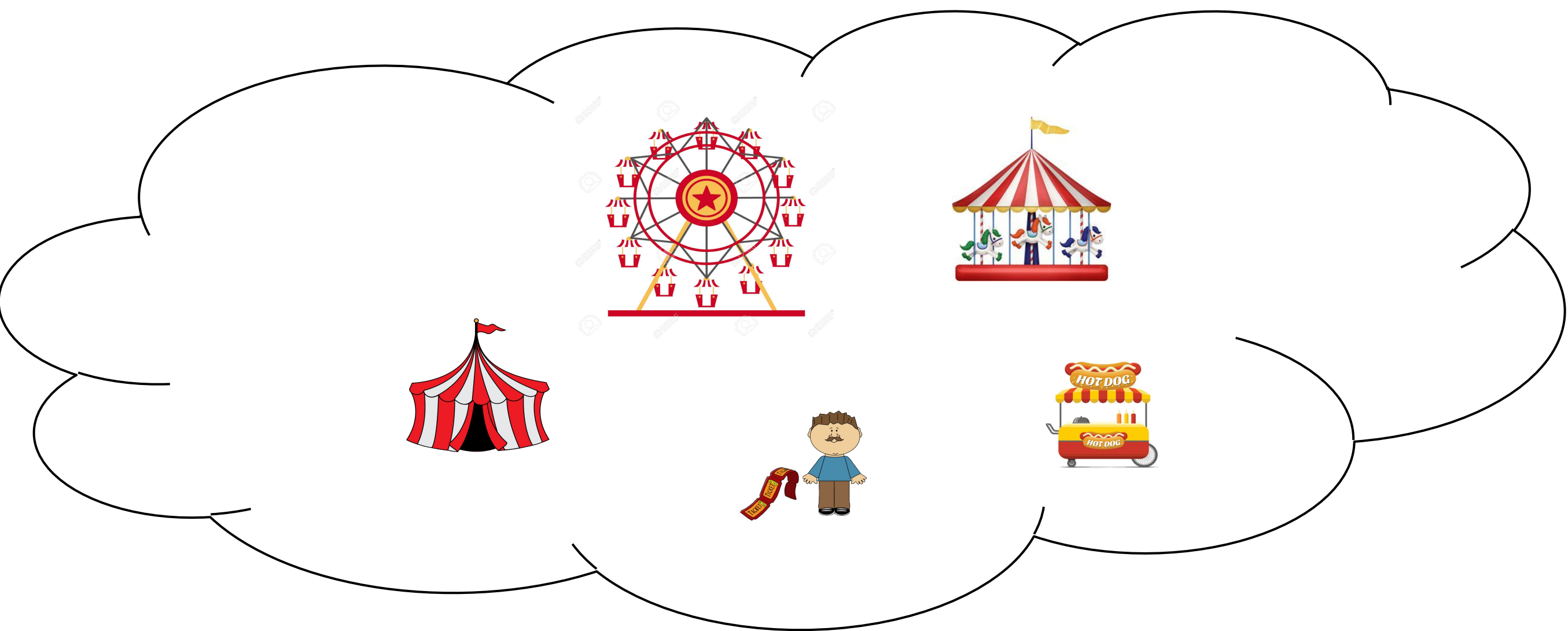


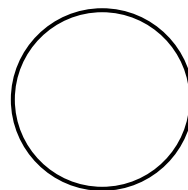
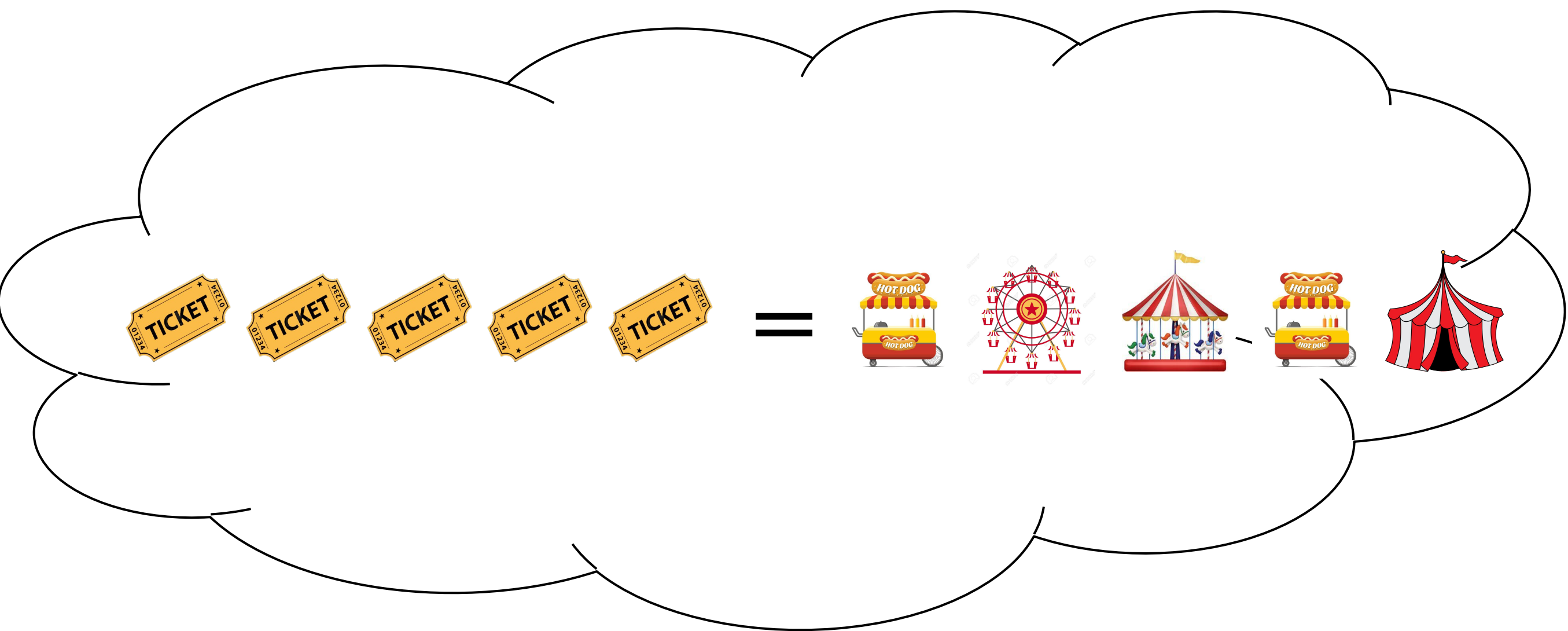


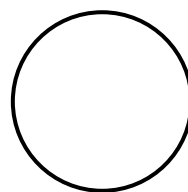
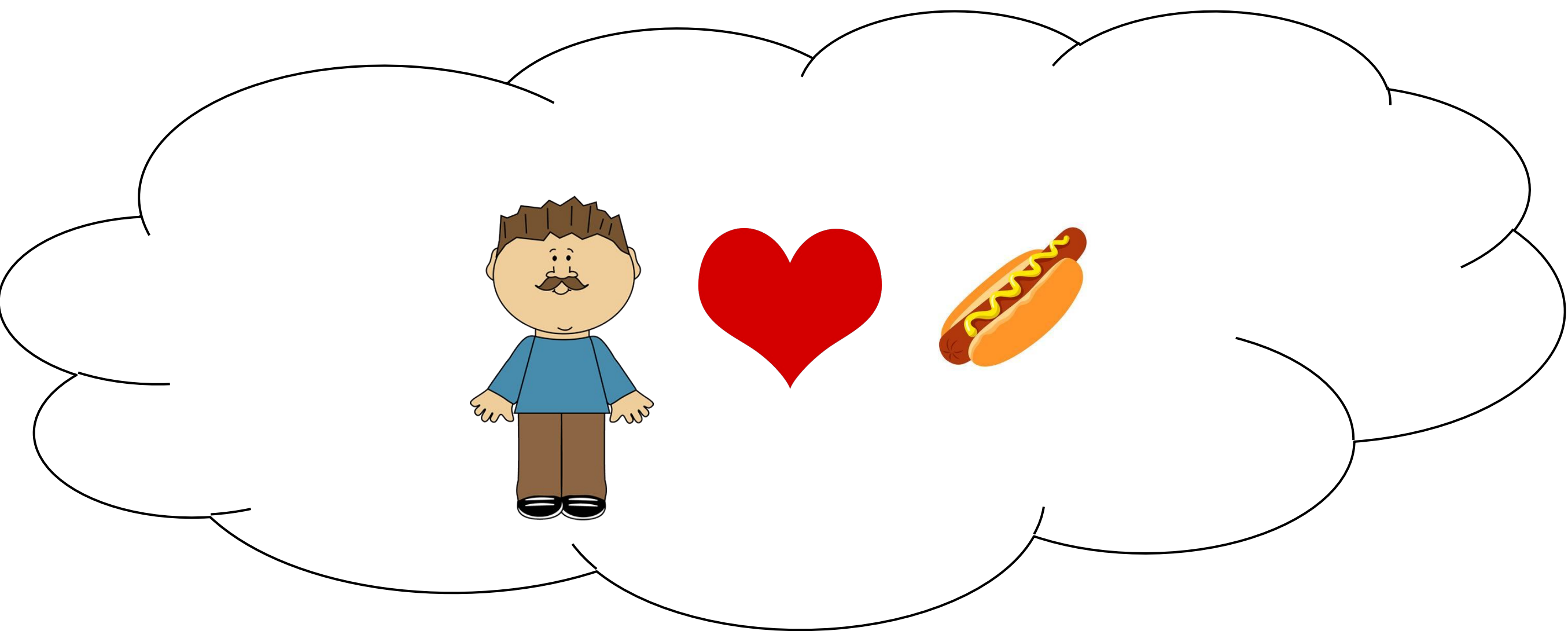












Why ZKAPs?

- ▶ Privacy problems with existing access-control (authorization) systems
- ▶ Example: ticket rolls:
 - Numbered labels to *authorize* ticket-holders
 - Corresponding “coupons” to *verify* disputes
 - Weakly “fungible”
 - But also:
 - A residual record of activity
 - A means of identifying individuals



Why ZKAPs?

- ▶ *ZKAPs can be used to authorize individual actions without identifying individual users*

Why ZKAPs?

- ▶ *ZKAPs can be used to authorize individual actions without identifying individual users*
- ▶ Uses batches of *blind signatures* as spendable “tokens”
 - Usage: Spend X tokens to perform resource-limited action Y
 - e.g. (PrivateStorage): spend X ZKAPs to store X MBs for 1 month
 - Tokens cannot be linked to token-holders or to each other
 - Tokens cannot be forged; issuance is controlled

Your Data, Your Control



Pay only for the space you actively use

Unlike other cloud storage providers, we feel you should not have to pay for storage space you are not actively using. In our system, you pay for the specific amount of space you use and for a set time span. If you wish to use more storage space, or use it longer, you simply use more of your PrivateStorage Credits.



Pay with anonymous tokens

PrivateStorage Credits work to control access to the storage service, while also maintaining our users' anonymity. By detaching a user's online activity from an 'account' or any specific payment methods, we make sure we do not know your identity.

Safe, Secure, Redundant, Recoverable

Should you lose access to your computer, then you can restore access to your data from another device, provided you have the Recovery Key. Your personal Recovery Key is a brief text file that contains only enough information to allow you to regain a connection to the storage grid and access any previously stored folders. It is critical to create a Recovery Key as soon as you start using PrivateStorage.

How Do They Work

Variable : Comment
Variable = Definition

See the greatest show
in the galaxy!

Satisfaction guaranteed!

- joe clown



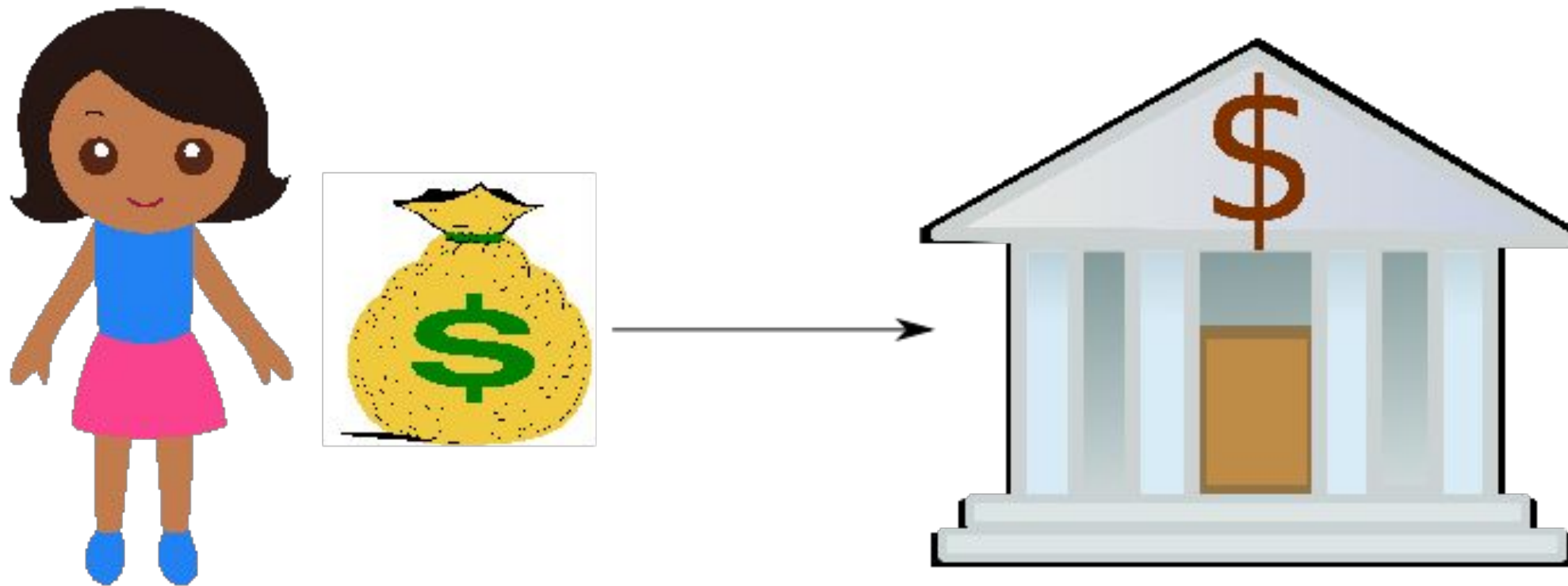
k : Secret key

Y : Public key

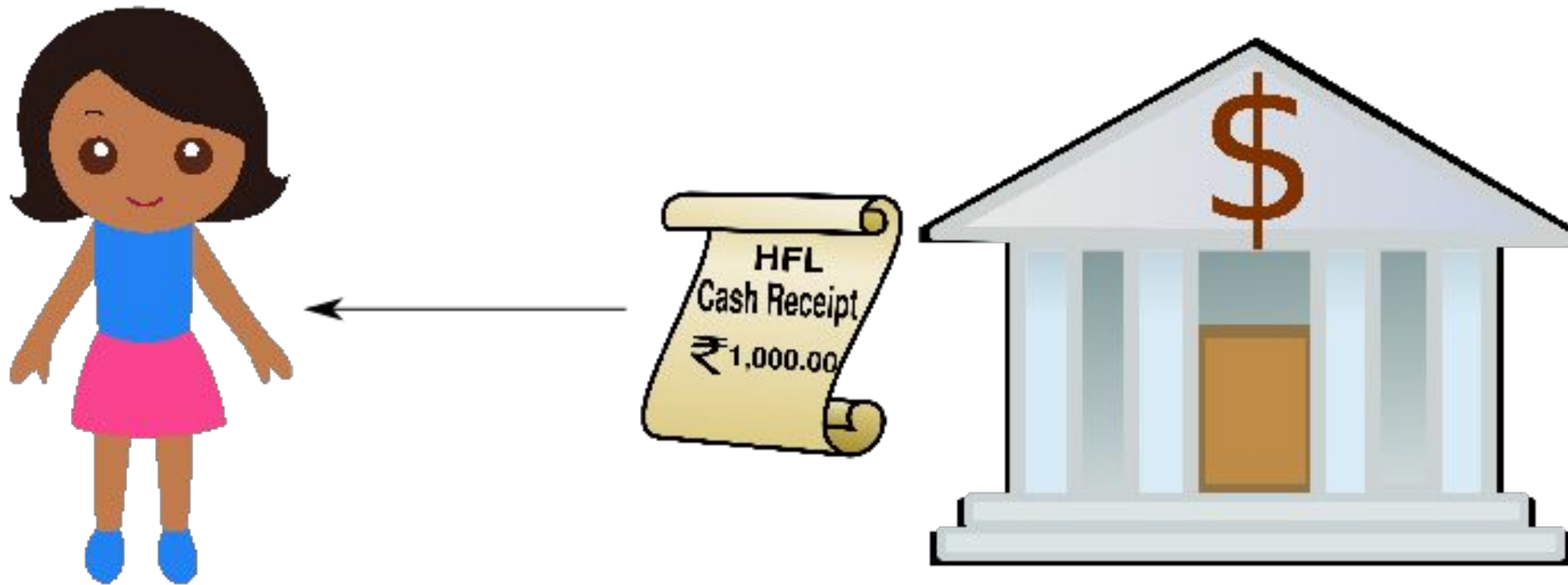
X : Ristretto point

$$Y = X^k$$

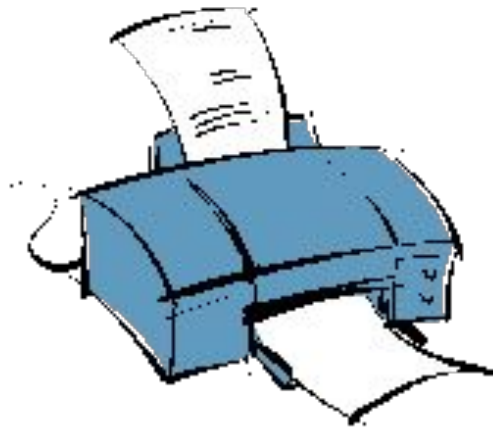
ZERO KNOWLEDGE ACCESS PASSES (ZKAPs)



ZERO KNOWLEDGE ACCESS PASSES (ZKAPs)



ZERO KNOWLEDGE ACCESS PASSES (ZKAPs)



t : Random preimage bitstring

T : Random token

$$T = H_1(t)$$

ZERO KNOWLEDGE ACCESS PASSES (ZKAPs)



P : Blinded token

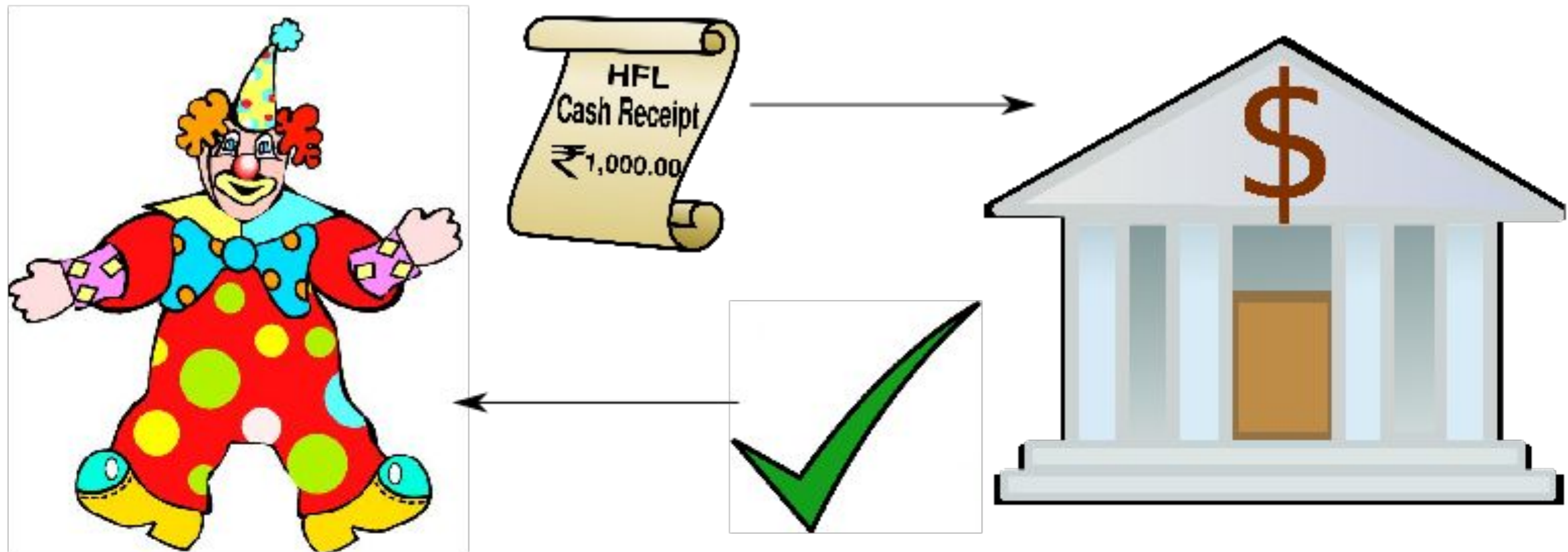
r : Random blinding scalar

$$P = T^r$$

ZERO KNOWLEDGE ACCESS PASSES (ZKAPs)



ZERO KNOWLEDGE ACCESS PASSES (ZKAPs)



ZERO KNOWLEDGE ACCESS PASSES (ZKAPs)



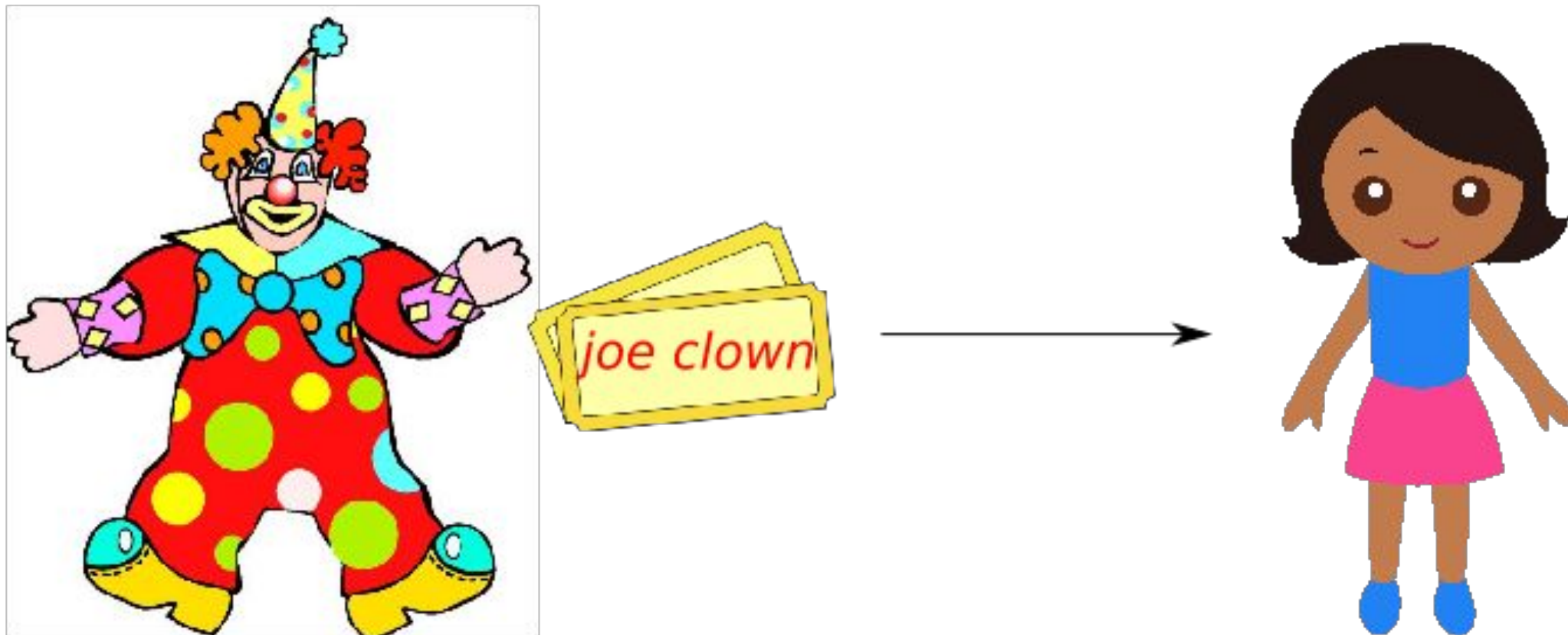
Q : Blinded signature

P : Blinded token

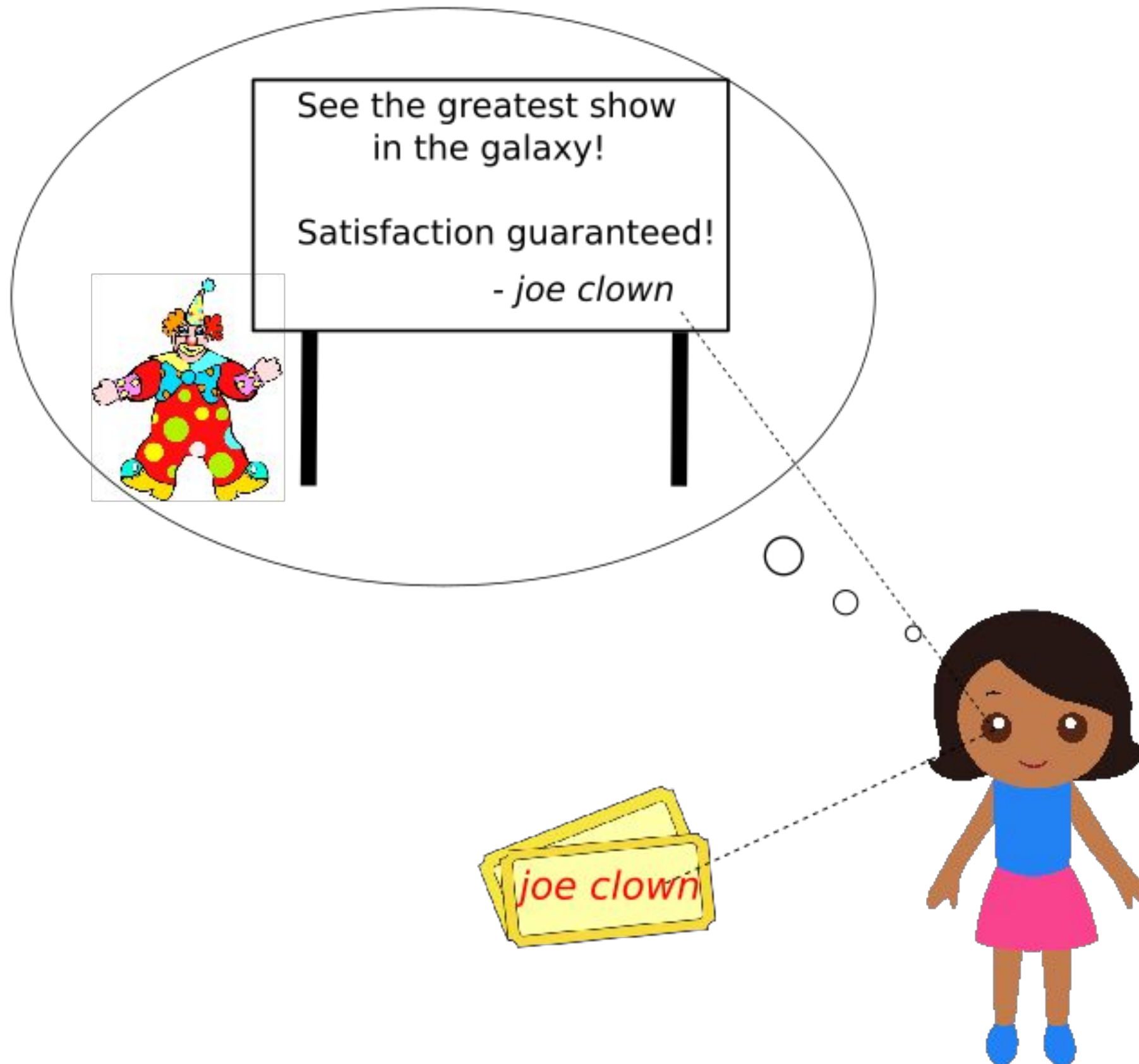
k : Secret key

$$Q = P^k$$

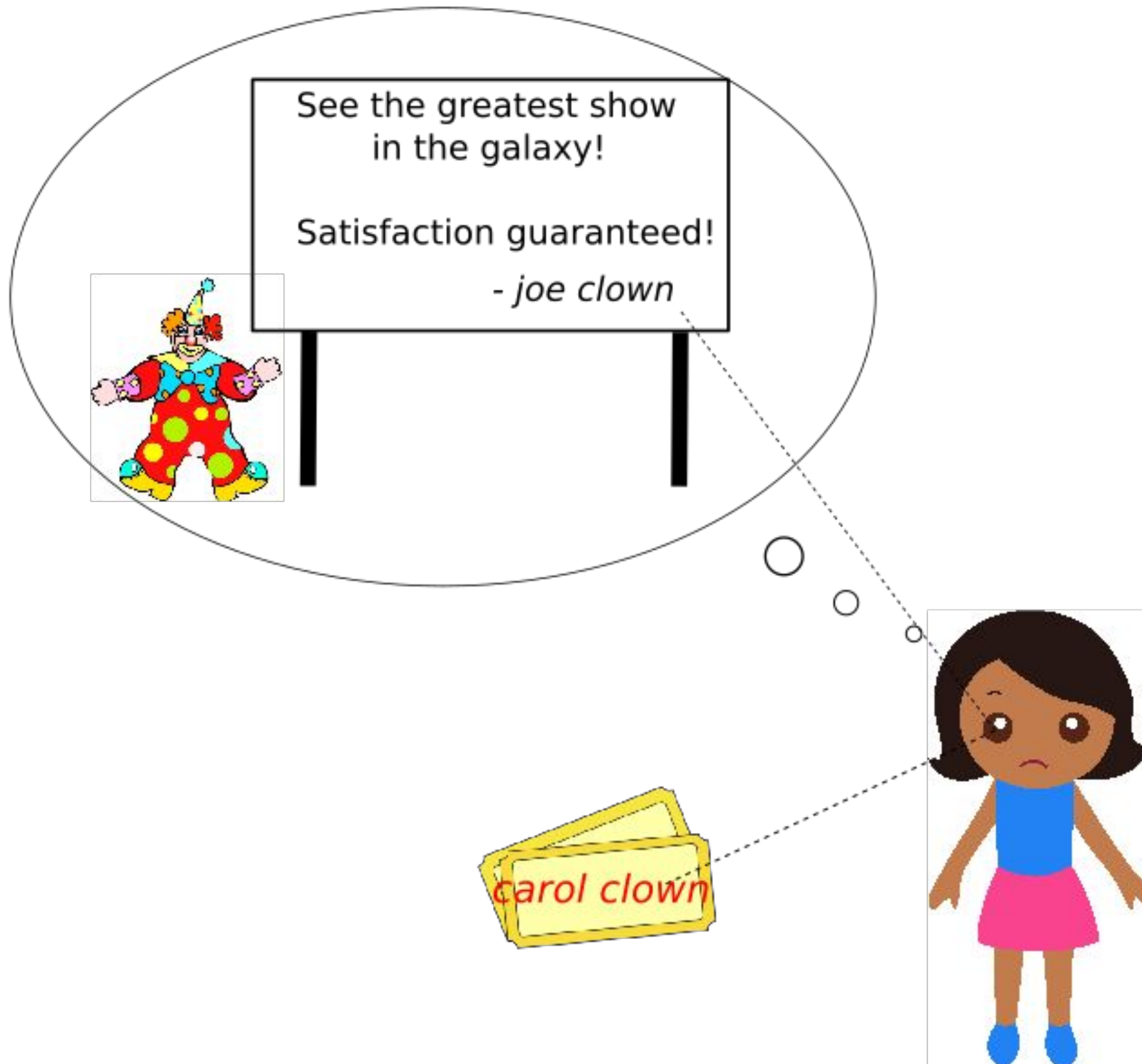
ZERO KNOWLEDGE ACCESS PASSES (ZKAPs)



ZERO KNOWLEDGE ACCESS PASSES (ZKAPs)



ZERO KNOWLEDGE ACCESS PASSES (ZKAPs)

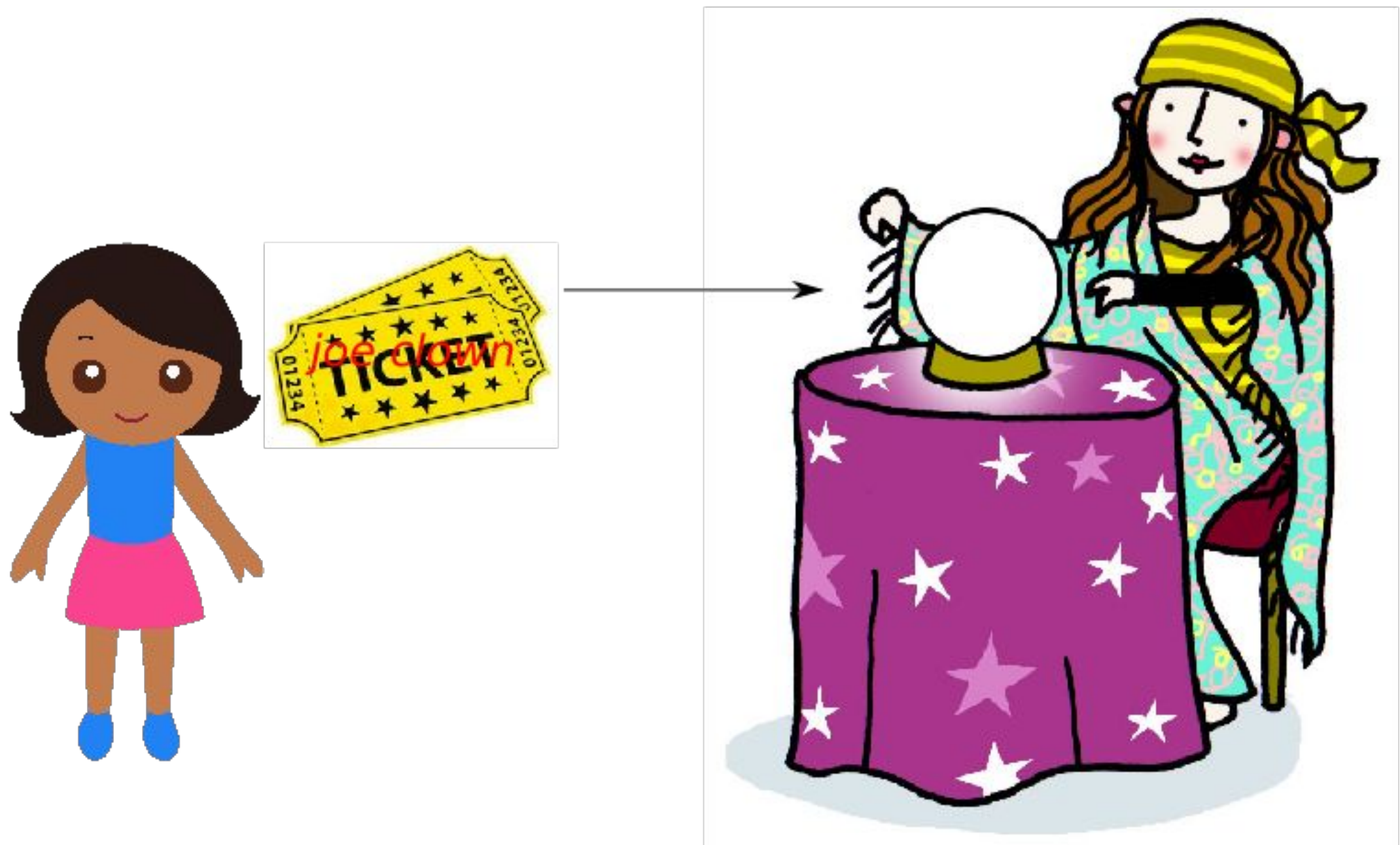


ZERO KNOWLEDGE ACCESS PASSES (ZKAPs)



W : Unblinded signature
Q : Blinded signature
r: Random blinding scalar
 $W = Q^{1/r}$

ZERO KNOWLEDGE ACCESS PASSES (ZKAPs)



K : Verification key

t : Random preimage bitstring

W : Unblinded signature

R : Message

$$K = H_2(t, W)$$

$(t, R, \text{MAC}_K(R))$: Access Pass

ZERO KNOWLEDGE ACCESS PASSES (ZKAPs)



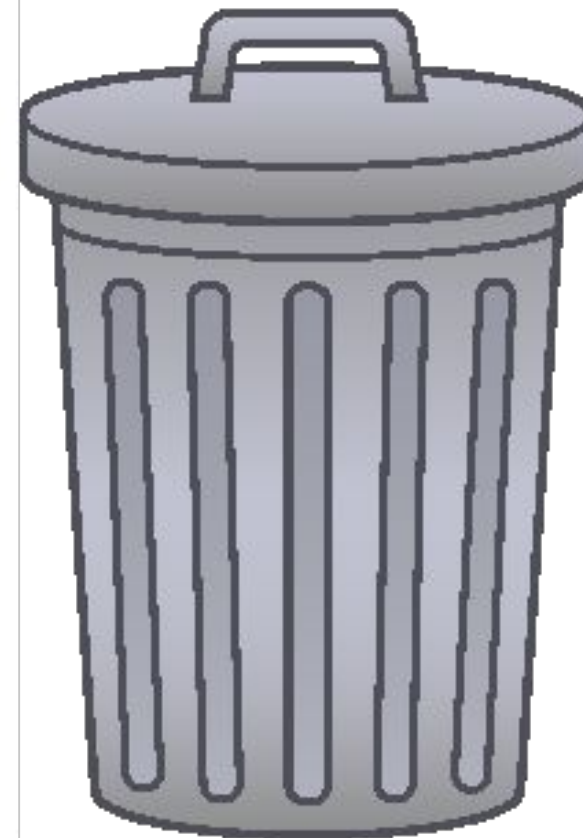
$$T' = H_1(t)$$

$$W' = (T')^k$$

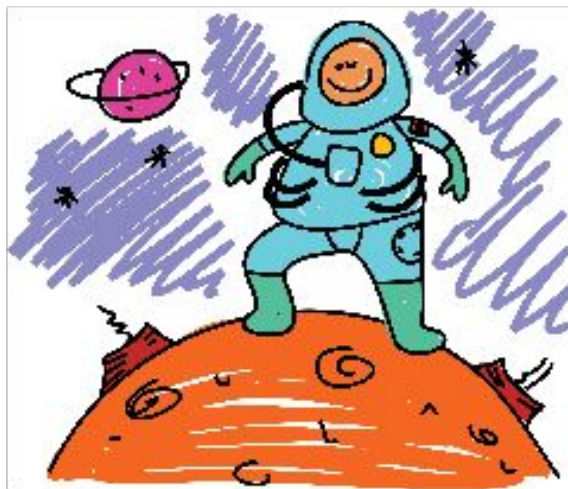
$$K' = H_2(t, W')$$

$$\text{MAC}_K(R) = ? \text{MAC}_{K'}(R)$$

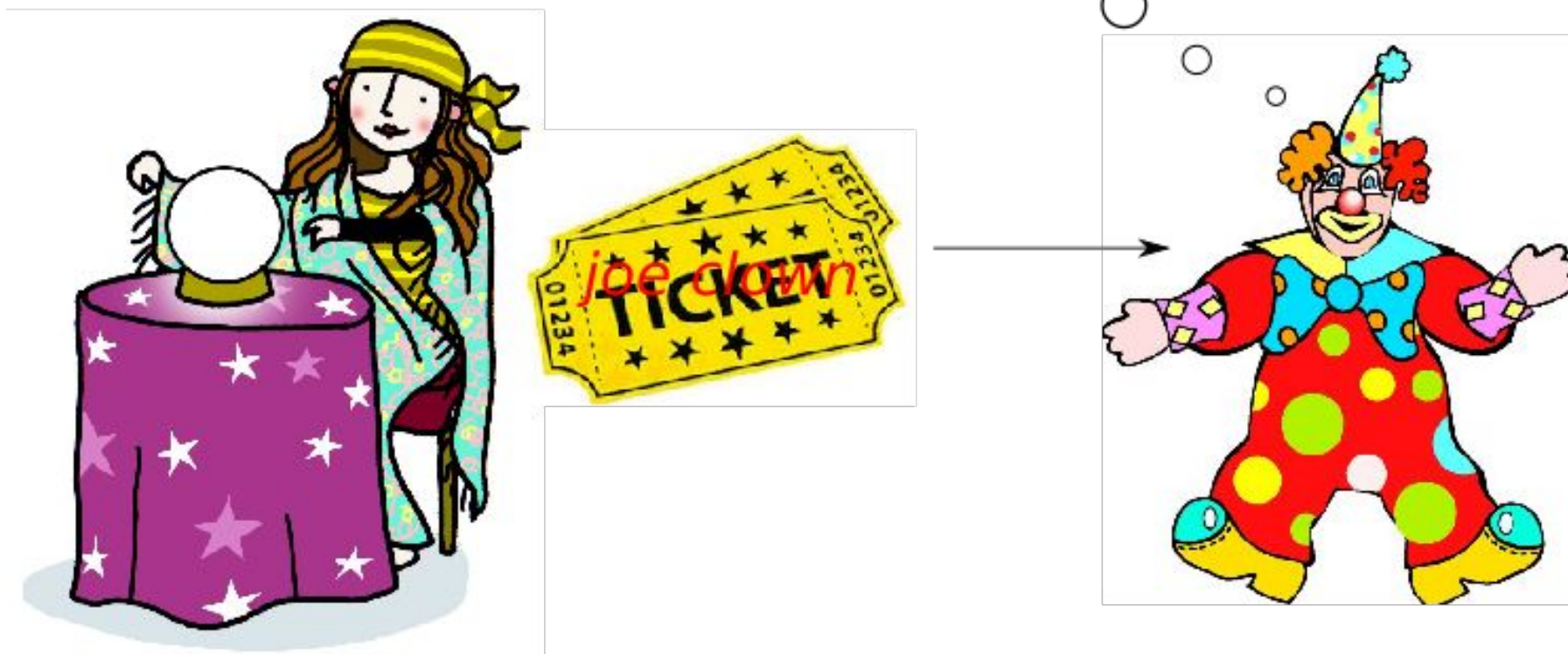
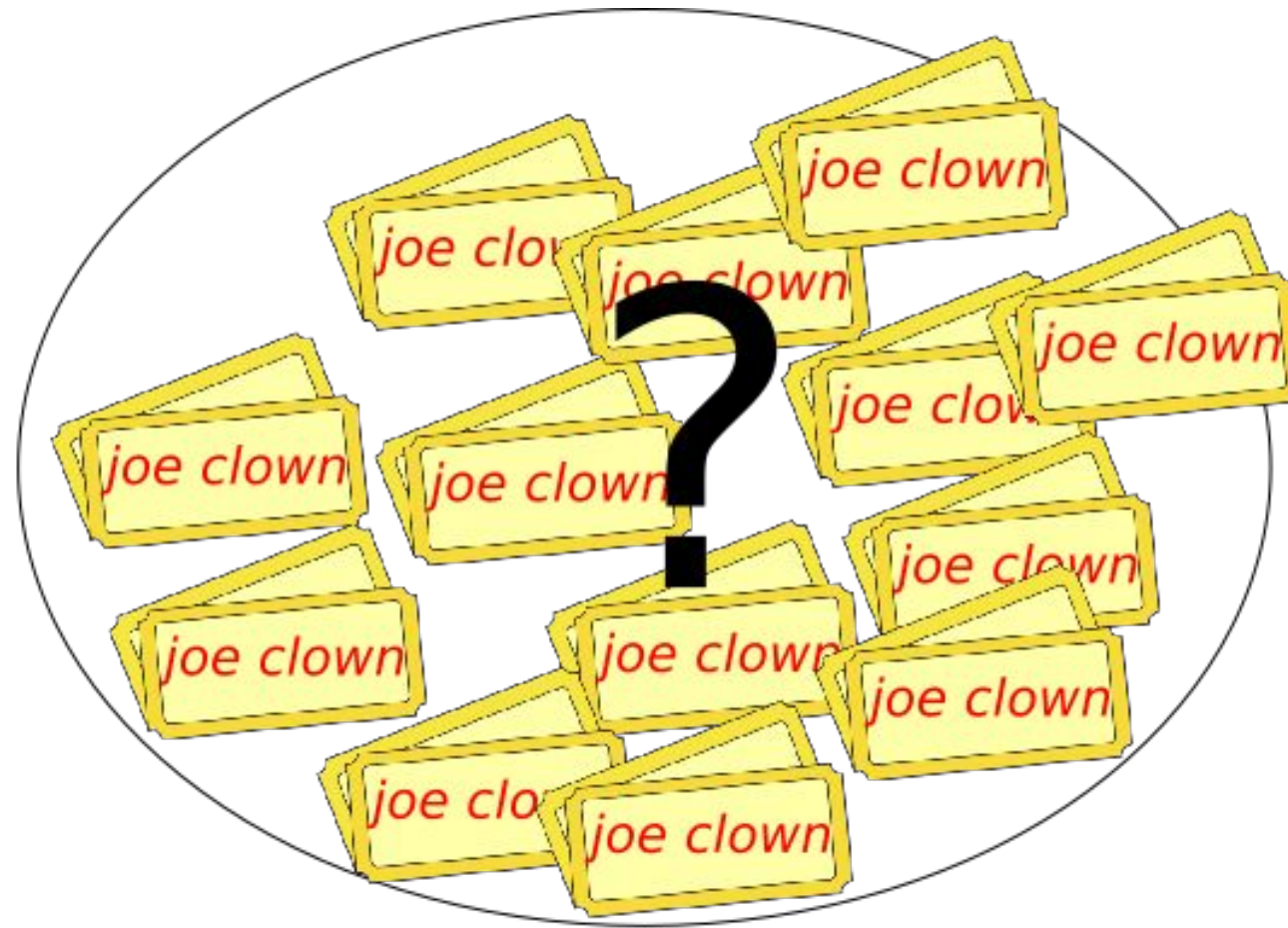
ZERO KNOWLEDGE ACCESS PASSES (ZKAPs)



ZERO KNOWLEDGE ACCESS PASSES (ZKAPs)



ZERO KNOWLEDGE ACCESS PASSES (ZKAPs)



Weaknesses

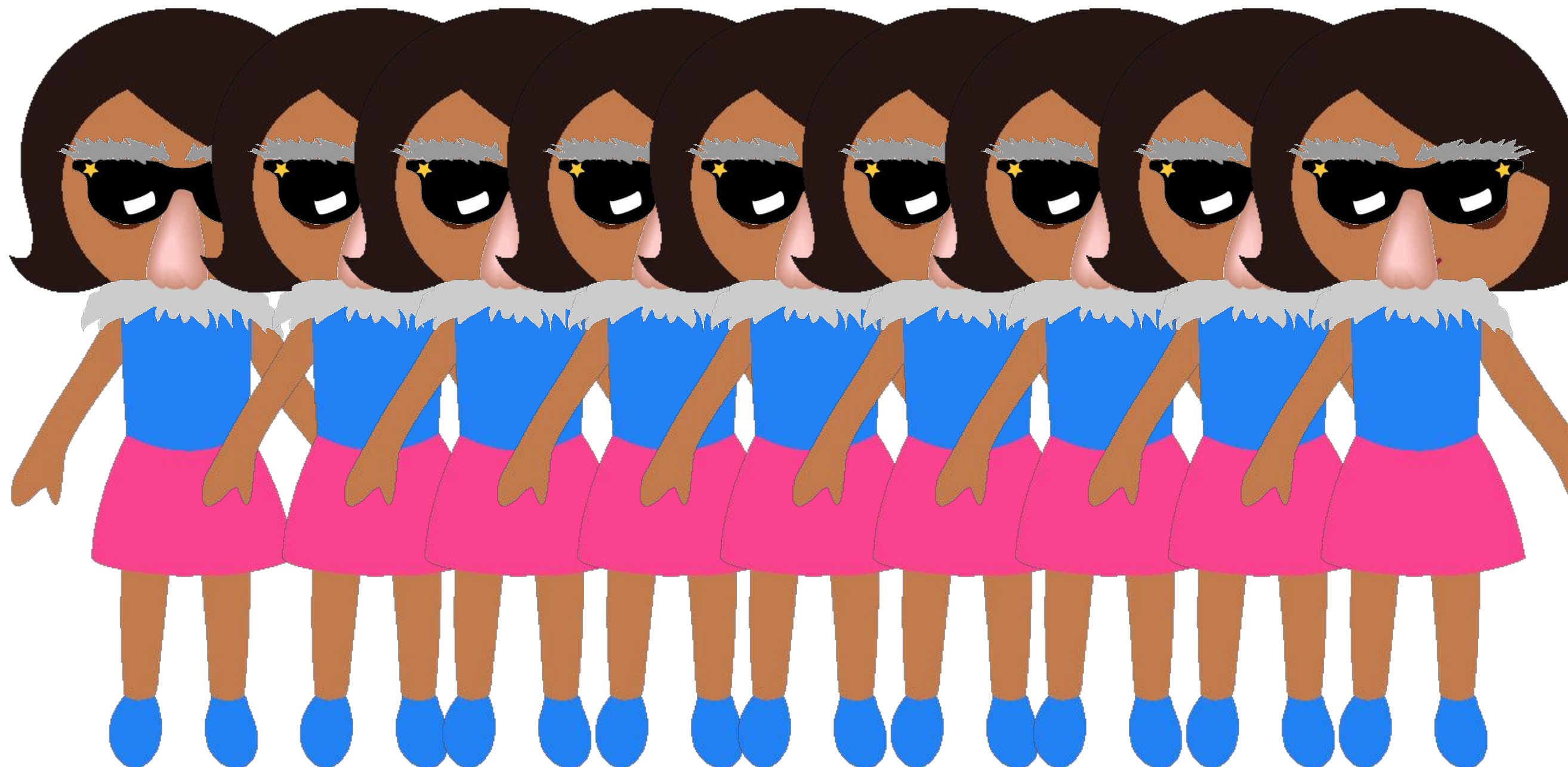
Single denomination



Metadata tracking



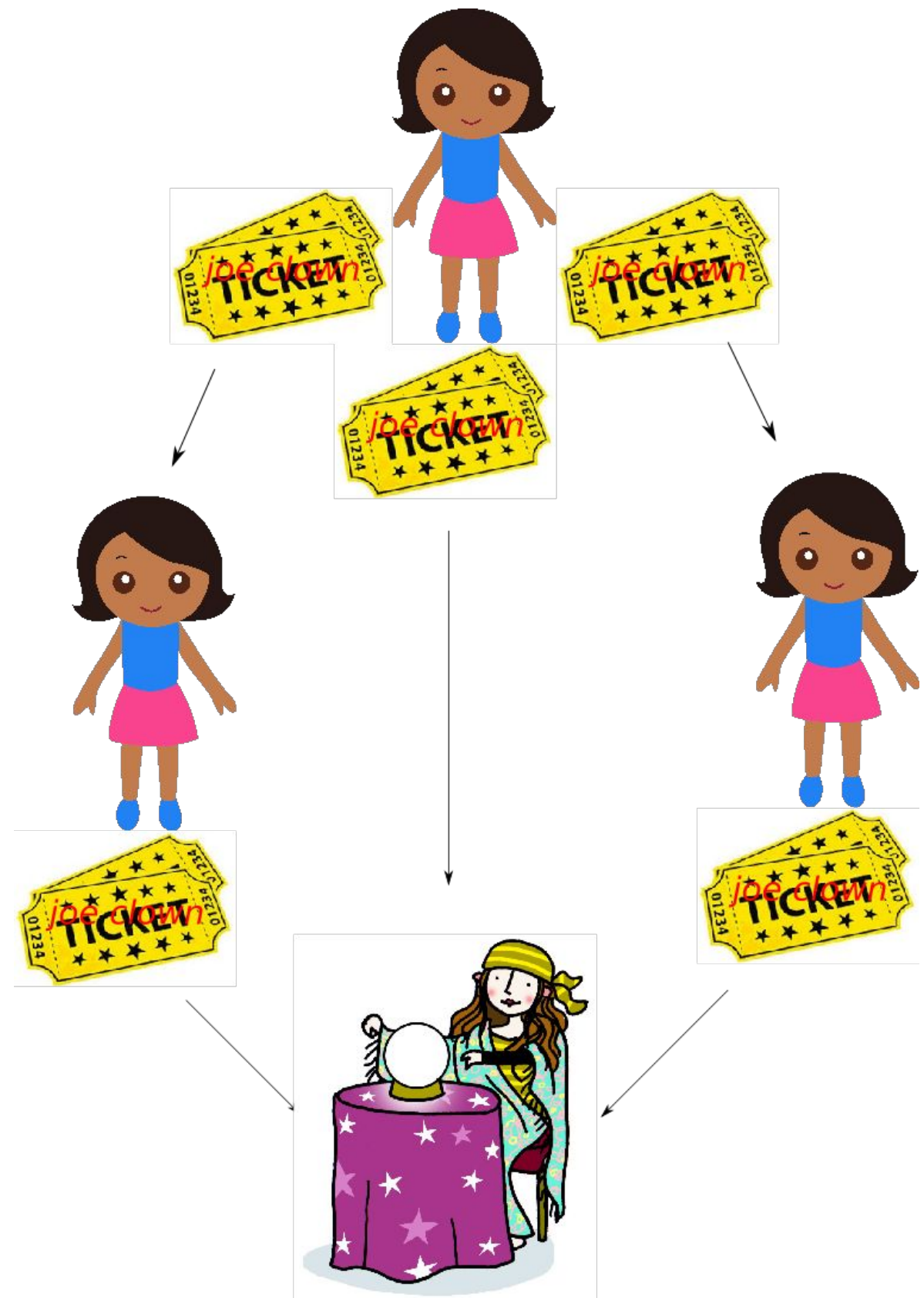
Necessity of a crowd



Other Use-Cases

Other Use-Cases

- Social media invites



Other Use-Cases

- ▶ Public transit credits
- ▶ VPN Service
- ▶ Identityless messaging service

Other Use-Cases

Relevant links / further reading

- ▶ <https://privatestorage.io/>
- ▶ <https://openprivacy.ca/assets/towards-anonymous-prepaid-services.pdf>
- ▶ <https://github.com/PrivateStorageio/ZKAPAuthorizer>
- ▶ <https://github.com/LeastAuthority/python-challenge-bypass-ristretto>
- ▶ <https://github.com/brave-intl/challenge-bypass-ristretto>
- ▶ <https://privacypass.github.io/>
- ▶ <https://www.petsymposium.org/2018/files/papers/issue3/popets-2018-0026.pdf>

Questions?

contactus@leastauthority.com