COM-402
Security and Privacy

Blockchains 2/3

Credits: some slides borrowed from Ari Juels

Cryptocurrency v0: SuckerCoin

Cryptocurrency v0: SuckerCoin
World of perfect trust

Pros / Cons of SuckerCoin (v0)

Pros:

- Dirt simple!
- Universal access
- Fast transactions

Cons:

- **No privacy**
- **No security**

Cryptocurrency v1: WallCoin
Registered digital currency

Cryptocurrency v1: WallCoin
Registered digital currency

- Trusted entity maintains *ledger*, i.e., all transactions over history of the system
  - E.g., running example: Facebuck
- Users identify themselves to Facebuck by logging into Facebuck's website
  - E.g., using password-based authentication
- Facebuck can dictate creation of money
  - E.g., users must deposit dollars with Facebuck


facebuck
3
3
4
Search
Home
Profile
Find Friends
facebuck$ wall
JP: $100
Dean Jim: $200
Transaction history:
Dean Jim ➔ JP : $50
14 May 2019
… (and all other users)
Logged in as Tsg BrickRed (Not You?)
Allow
Don't Allow
Facebook © 2011 · English (US)
About · Advertising · Create a Page · Developers · Careers · Privacy · T

facebuck

Search

Home Profile Find Friends

facebuck$ wall

JP: $100

Dean Jim: $200

JP: $150

Dean Jim: $150

… (and all other users)

Transaction history:

- Dean Jim ➔ JP : $50
- 14 May 2019

JP liked this

Logged in as Tsg BrickRed (Not You?)

Allow Don't Allow

Pros / Cons of WallCoin (v1)

Pros:

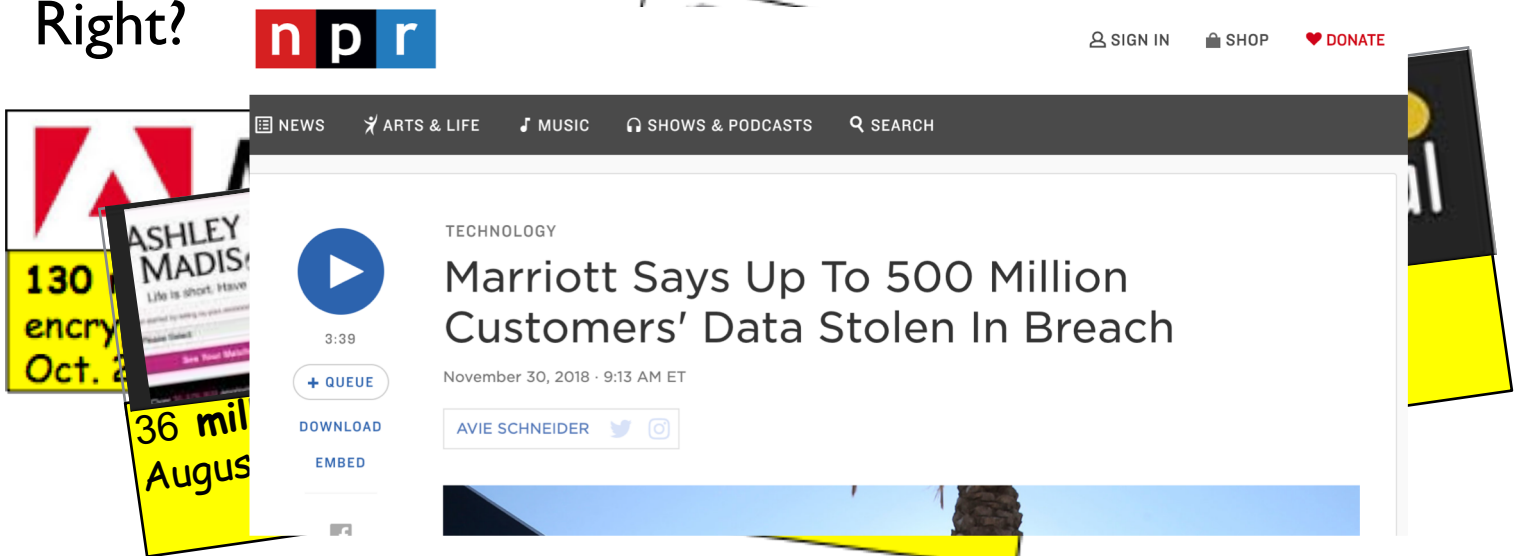
- Dirt simple!
  - (At least simpler than Facebook privacy settings)
- Universal access
- Fast transactions
- Facebuck can fix errors / reverse transactions

Cons:

- No privacy
  - Facebuck could show information selectively, but…
- **Weak security**

Weak security?

- What if Facebuck cheats?
  - E.g., forges Dean Jim ➔ JP: $100
- If Facebuck shows wall selectively for privacy, more opportunity to cheat
- What if passwords are stolen from the system? Unthinkable! Right?

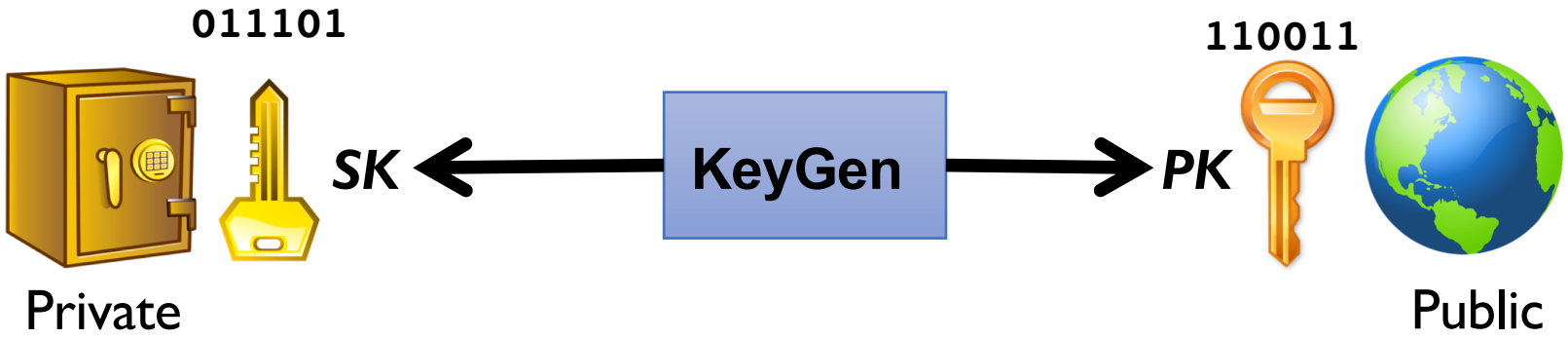


Transaction authentication

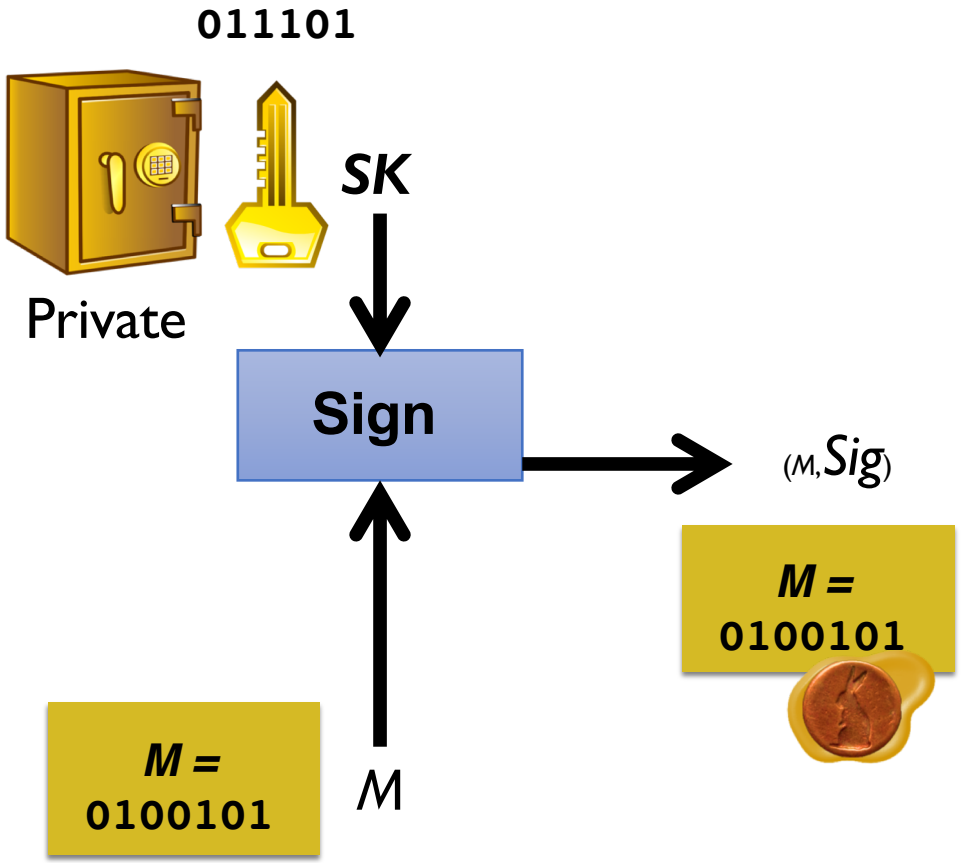
- Passwords represent tradeoff
  - Convenient but vulnerable
  - Require Facebuck to manage them
- Alternative: Digital signatures
  - Much stronger security
  - Facebuck can verify that I authorized a transaction without knowing my secrets!

Digital Signatures: Quick Reminder

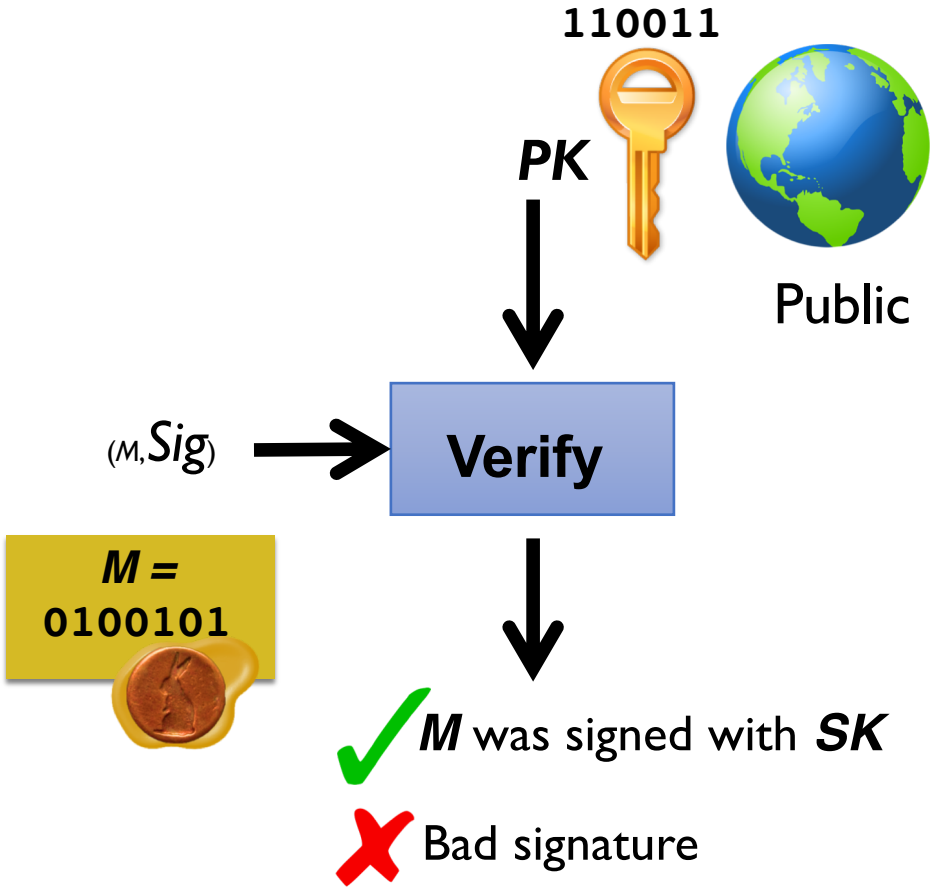
Digital signatures



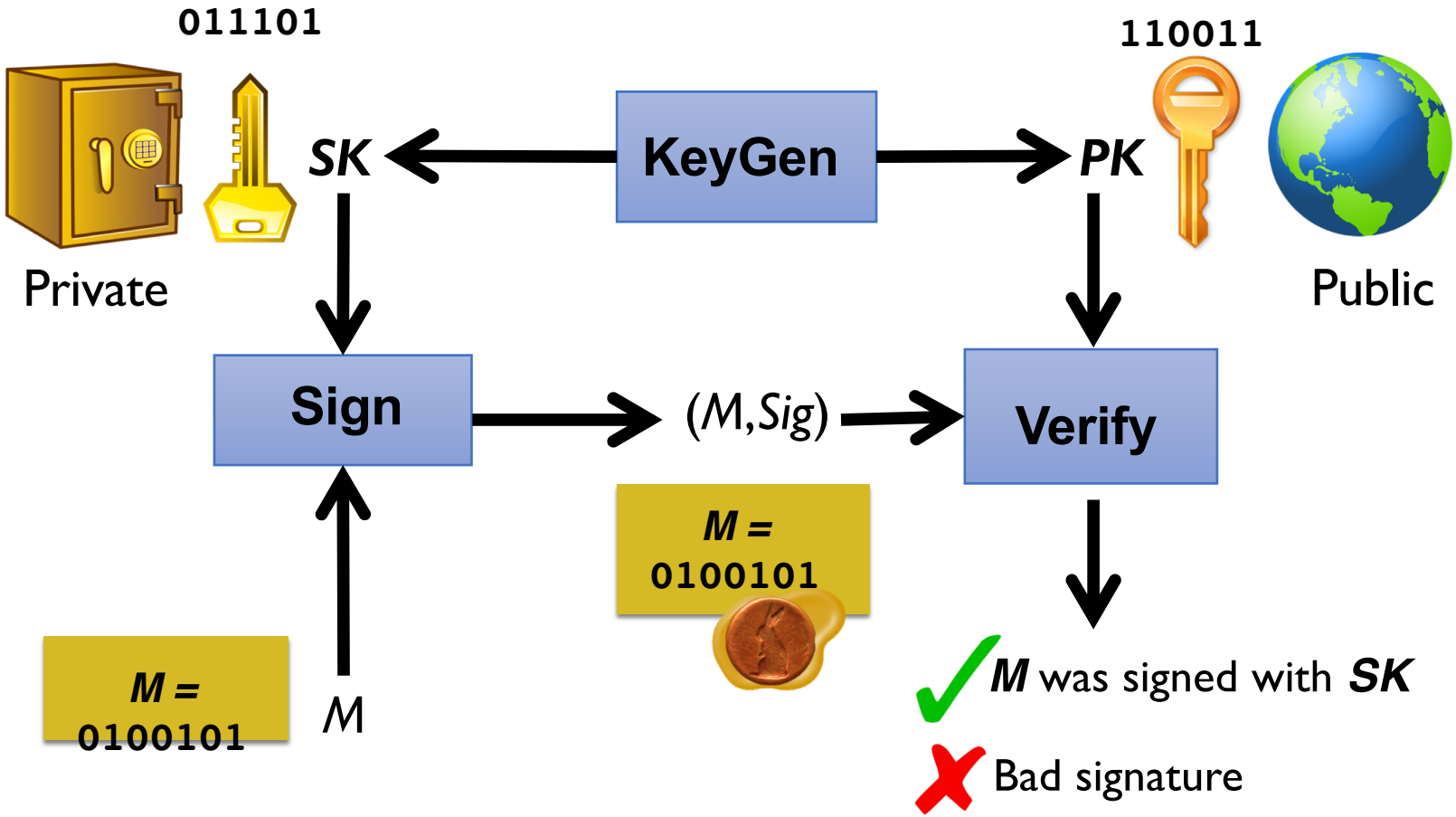
Digital signatures: Technical view



Digital signatures: Technical view



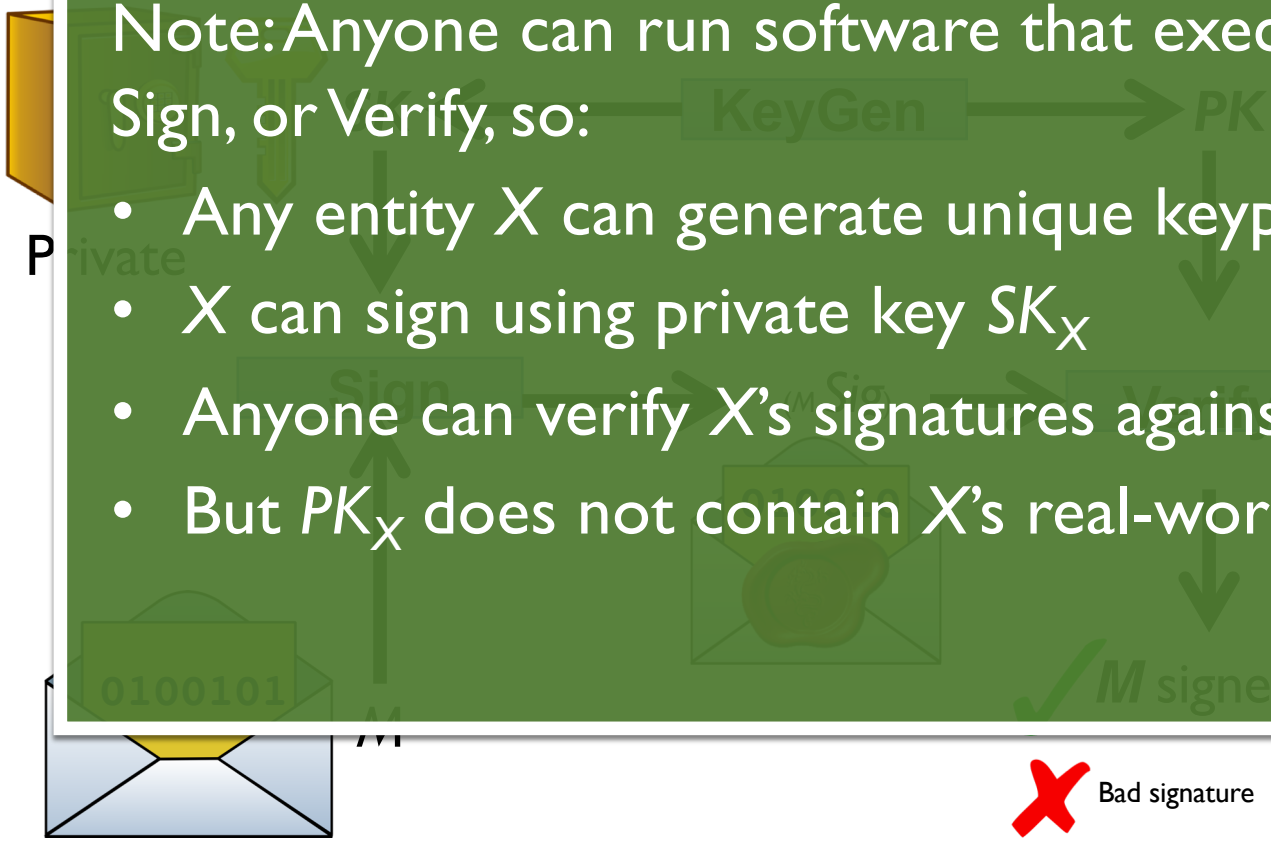
Digital signatures: Technical view



Digital signatures:

Note: Anyone can run software that executes KeyGen, Sign, or Verify, so:

- Any entity *X* can generate unique keypair (SK_X, PK_X)
- *X* can sign using private key SK_X
- Anyone can verify *X*'s signatures against PK_X
- But PK_X does not contain *X*'s real-world identity



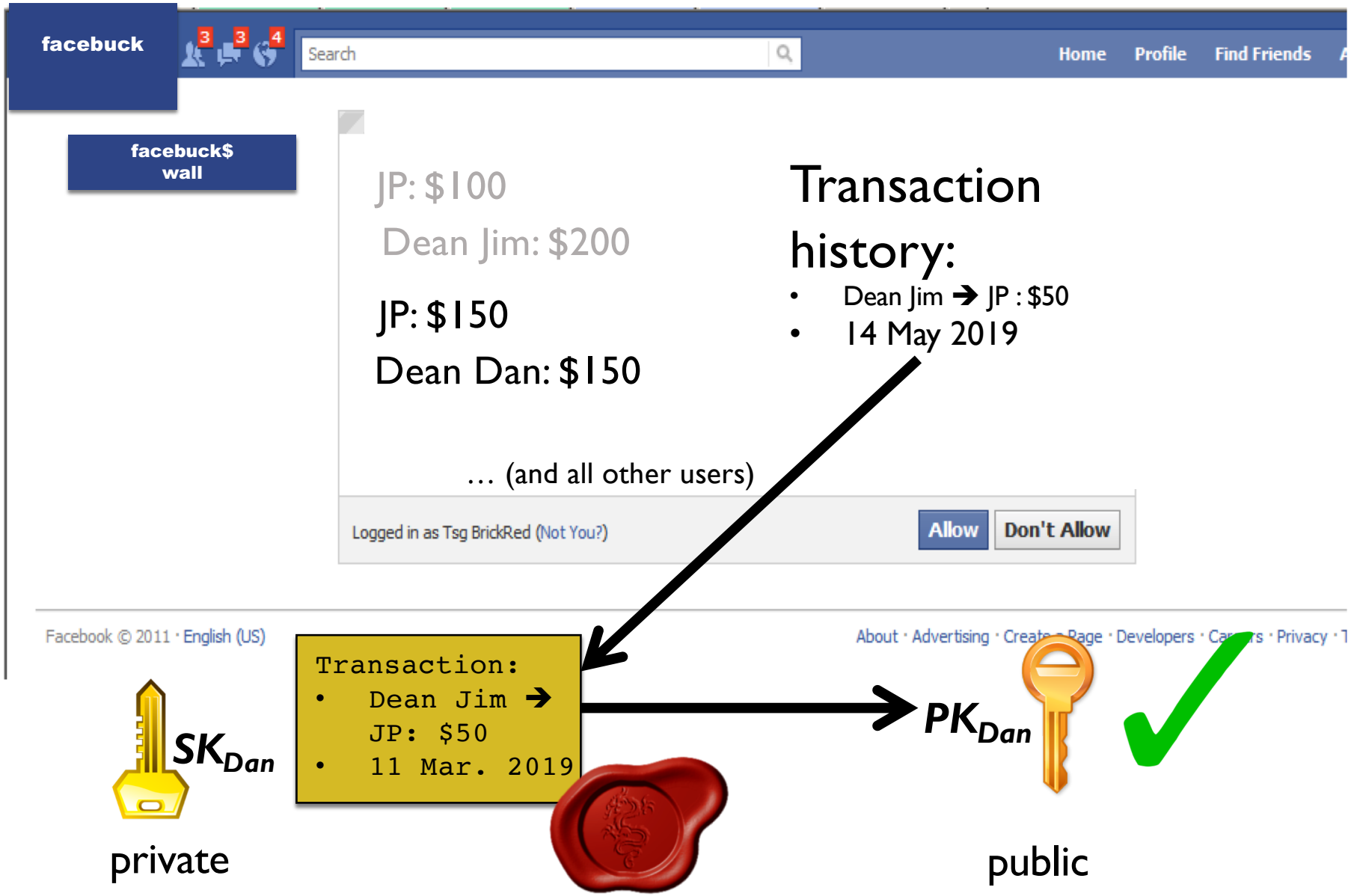
Bitcoin uses ECDSA

- "Elliptic-Curve Digital Signature Algorithm"
- Private key *SK* is 256 bits (32 bytes); (compressed) public key *PK* is 33 bytes
- secp256k1 (slightly nonstandard) curve

Cryptocurrency v2: SigCoin

Cryptocurrency v2: SigCoin

- For every account *X*, sign transactions using private key SK_X
- Assume all public keys PK_X known to the world


facebuck
Search
Home
Profile
Find Friends
facebuck$ wall
JP: $100
Dean Jim: $200
JP: $150
Dean Dan: $150
Transaction history:
• Dean Jim → JP : $50
• 14 May 2019
… (and all other users)
Logged in as Tsg BrickRed (Not You?)
Allow
Don't Allow
Facebook © 2011 · English (US)
About · Advertising · Create a Page · Developers · Careers · Privacy
Transaction:
• Dean Jim → JP: $50
• 11 Mar. 2019
SK_Dan
PK_Dan
private
public

Better security!

- Facebuck can't falsify my transactions
- Without SK_{Dan}, no way to generate valid transaction signature
- SK_{Dan} can't be stolen from Facebuck
  - It's not on the Facebuck server!

Adding privacy

- Users can be identified using public keys, not real-world identifiers
  - E.g., JP is known to Facebuck as PK_X
- Users are now *pseudonymous*
  - Transactions linkable, so only partial privacy
    - *X* $➔ *Y, Z*
- What are risks of pseudonymity?
  - E.g., if someone learns that PK_X is Ari, Ari loses his privacy

Pros / Cons of SigCoin (v2)

Pros:

- No passwords to steal
- Universal access
- Fast transactions
- Facebuck can't falsify transactions

Cons:

- Users need to manage private keys
  - Can't store in head like password!
- Facebuck needs to manage public keys
- Partial privacy: Pseudonymity only
- **Facebuck can still cheat**

Private key *SK* = ownership
leakage = theft

How can Facebuck still cheat?

- Can fail to process / post transactions
  - E.g., Facebuck has a put option on an equity—delays or suppresses buy orders by customers
  - E.g., govt. pressures Facebuck to block transactions of suspected criminal
- Can go back and erase transactions!
  - Can take away your money
- Can show different subsets of transactions to different users
- *Rare events, but if they happen, you could lose everything!*

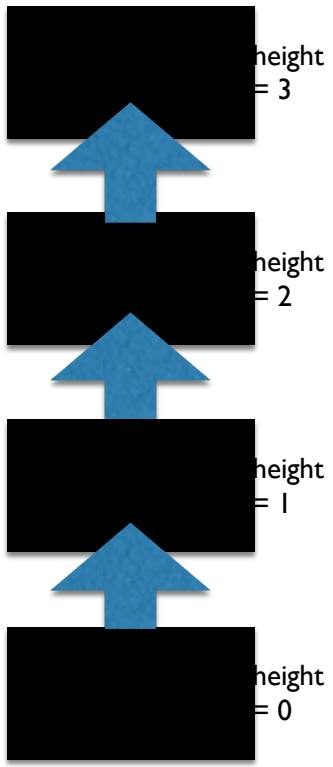
Cryptocurrency v3: ChainCoin

Cryptocurrency v3: ChainCoin

- Facebuck periodically—*every 10 minutes*—digitally signs batches of transactions (linked to old batches)
- Facebuck publishes batch for users to see and record
- Now:
  - Batches of transactions signed w.r.t. $PK_{Facebuck}$
  - If Facebuck presents different batches to different users, will be caught
  - If Facebuck tries to delete transaction after the fact, will get caught

Ledger now constructed as a chain of *blocks*

- A *block* is a batch of transactions + a digital signature
- Whole chain contains all transactions over time
- This is a *blockchain*
- Specifies complete system history



Pros / Cons of ChainCoin (v3)

Pros:

- Facebuck can't falsify transactions
- No passwords to steal
- Universal access
- Fast transactions
- If Facebuck deletes transaction, will get caught
- If Facebuck "forks," will get caught

Cons:

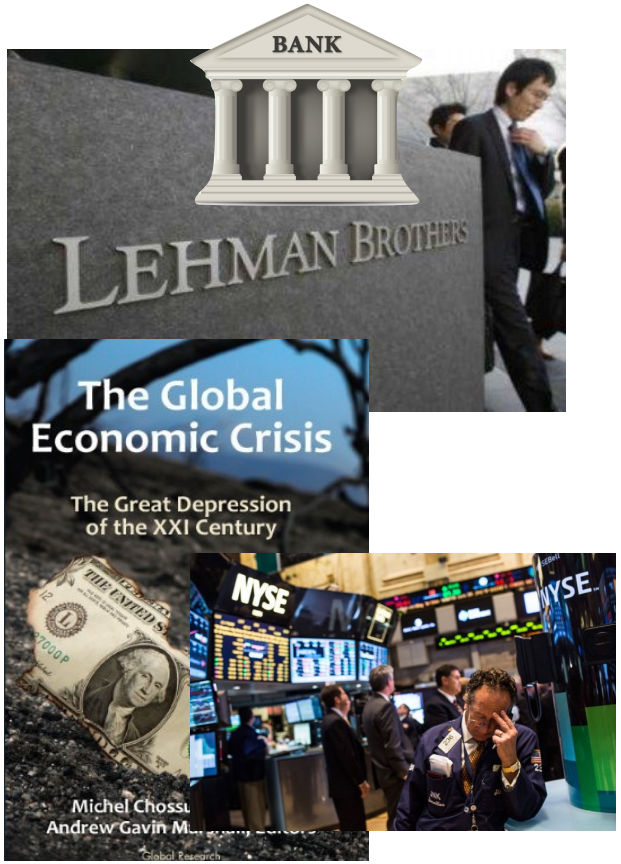
- Users need to manage private keys
  - Can't store in head like password!
- Facebuck needs to manage public keys
- Partial privacy: Pseudonymity only
- **Facebuck can suppress transactions**

Transaction suppression

- Facebuck can refuse to process / post transactions
- If Facebuck cheats, there's no recourse
  - You catch Facebuck cheating, not much you can do
- Trust resides in a single entity

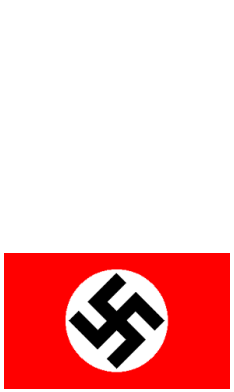
Why not trust a central authority?

- E.g., we all trust big banks to manage our money, right?



Why not trust a central authority?

- Hyperinflation, e.g.,
  - Germany in 1919-23 →
  - Zimbabwe: 624% in 2004



- Frozen assets, e.g.,
  - Greece: banks closed for a week in 2015
  - Argentina: Forbade purchase of dollars from 2011-4

Bitcoin

The Consensus Problem

Bitcoin

- Just like ChainCoin, i.e.,
  - Pseudonymous: User identities correspond to (*SK*, *PK*) key pairs
  - Users digitally sign transactions to authorize movement of money
  - Transactions recorded in blockchain

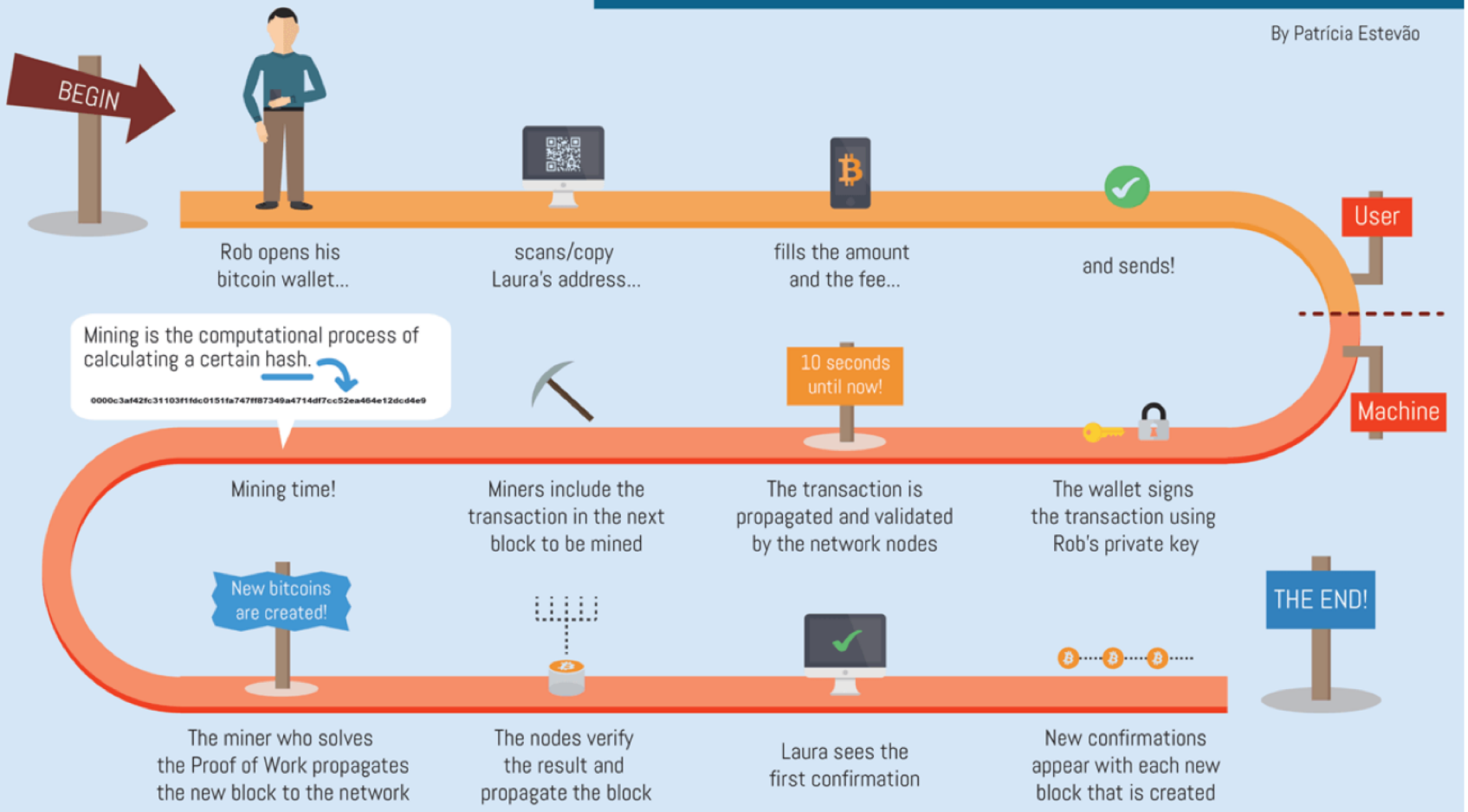
Bitcoin

- Except that the blockchain is *fully decentralized*
- Instead of *one* trusted entity like Facebuck, we rely on *whole community*
- Community maintains fully public blockchain / ledger, so that…
- No bank or jurisdiction can suppress transactions

THE BITCOIN TRANSACTION LIFE CYCLE

Rob's quest to send 0.3 BTC to his friend Laura

By Patrícia Estevão



How does community agree on what transactions in ledger?

This is the problem of ***consensus***