Countermeasures against Government-Scale Monetary Forgeries

Alessandro Acquisti, Nicolas Christin, Bryan Parno, Adrian Perrig

Carnegie Mellon University

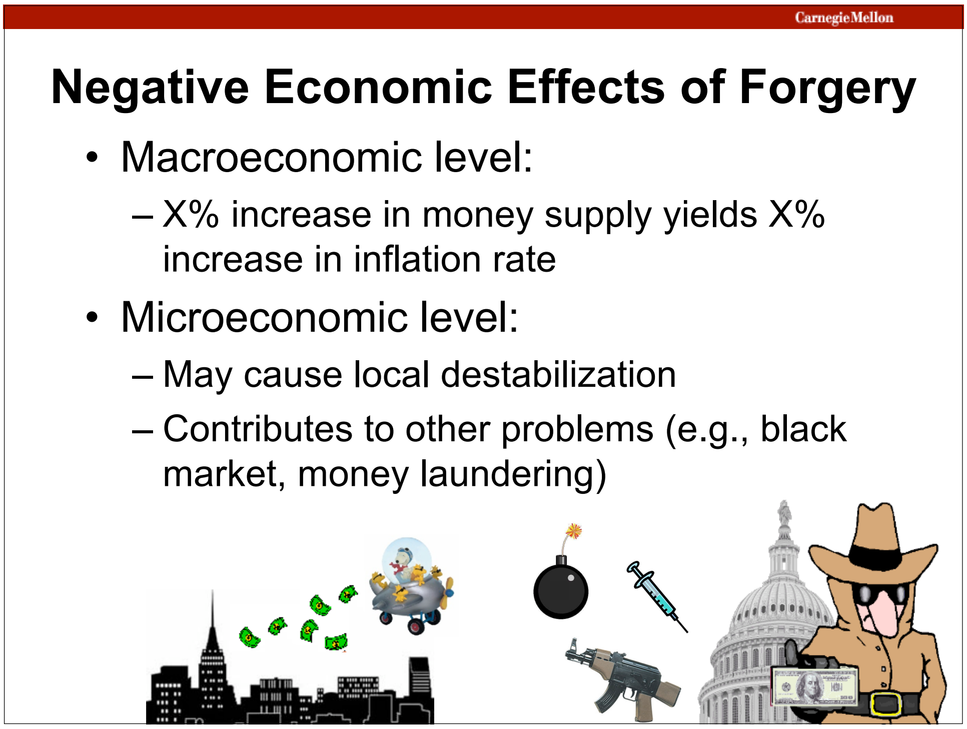
January 31, 2008

Government-Scale Monetary Forgeries

- **Nearly-perfect** fake U.S. dollar bills have appeared on a significant scale (NY Times)
- Experts suspect the forgeries are **government-mandated**
- New threat model
  - **Scale:** Attacker’s resources comparable to victim’s
  - **Motivation:** Theft or destabilization
  - **Perception:** Attack on national sovereignty

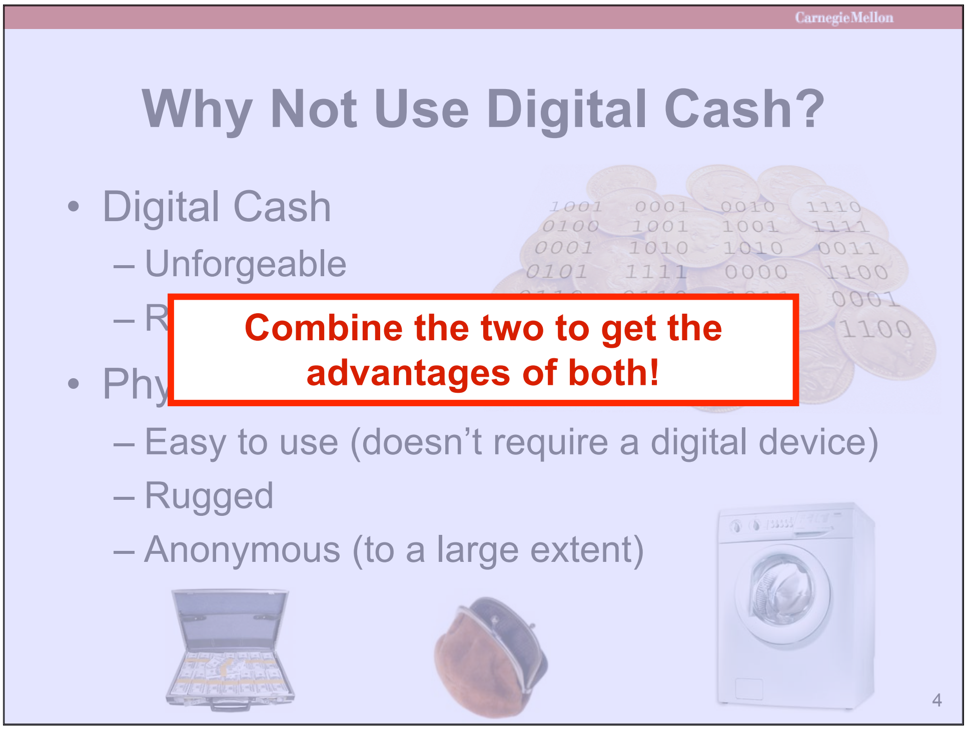
Should we do something?

Can we do something?



Negative Economic Effects of Forgery

- Macroeconomic level:
  - X% increase in money supply yields X% increase in inflation rate
- Microeconomic level:
  - May cause local destabilization
  - Contributes to other problems (e.g., black market, money laundering)



Why Not Use Digital Cash?

- Digital Cash
  - Unforgeable
  - R
- Phy
  - Easy to use (doesn't require a digital device)
  - Rugged
  - Anonymous (to a large extent)

Combine the two to get the advantages of both!

Physical Digital Cash Requirements

Universal use	Rugged bills that can be used anywhere
Forgery proof	Impractical to fake new bills
Useless duplication	Existing bills cannot be copied
Universal verifiability	Bills can be verified anywhere
Simple upgrade	Countermeasures integrate seamlessly
Reusability	Bills can be used more than once
Anonymity	Bill exchanges cannot be traced

Properties: Existing Solutions

	Traditional Cash	Digital Cash
Universal use	√	✗
Forgery proof	✗	√
Useless duplication	✗	√
Universal verifiability	?	✗
Simple upgrade	√	✗
Reusability	√	✗
Anonymity	√	?

Three-Layered Solution

2-D Barcode Signatures

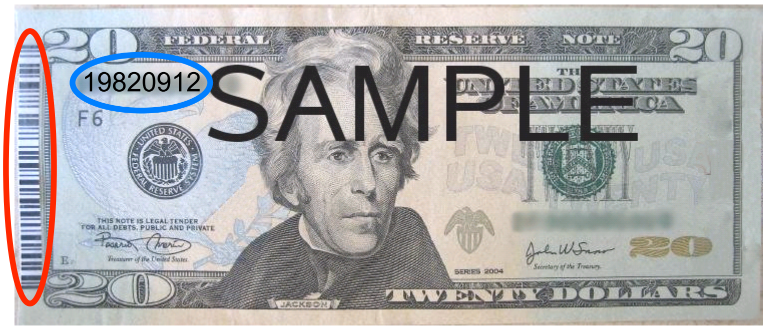
+

Online Verification

+

Physical One-Way Functions

2-D Barcode Signatures



- Bar code = Sign(Seq. number, Treasury Private Key)
- Creating new bills extremely difficult (with secure signature scheme)
- Production cost negligible

Signature Verification

Signature (bar code) can be verified optically with low-end equipment using the (widely publicized) Treasury's public key

Verification can be automated in bill counters too!

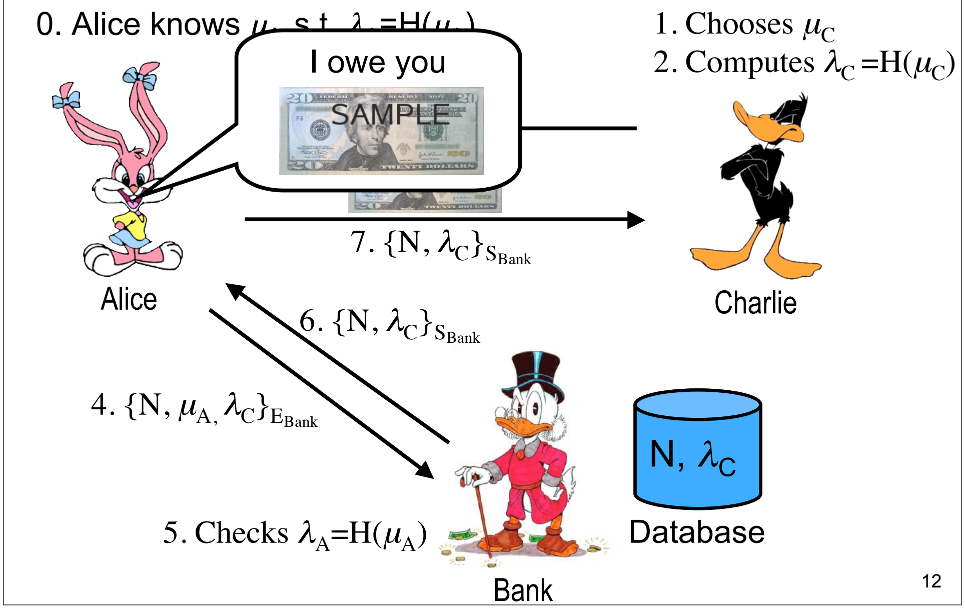
Properties: 2-D Barcodes

	Traditional Cash	Digital Cash	2-D Barcodes
Universal use	√	✗	√
Forgery proof	✗	√	√
Useless duplication	✗	√	✗
Universal verifiability	?	✗	√
Simple upgrade	√	✗	√
Reusability	√	✗	√
Anonymity	√	?	√

Online Verification

- Bank maintains a database
  - May be centralized or distributed
- Database associates each bill’s sequence number with a “lock value” λ
- Only current owner can unlock a locked bill
  - Reveals private value μ
- During transfer, current owner unlocks the bill, and allows new owner to lock it
  - Legacy users simply use unlocked bills

Example Implementation



0. Alice knows μ_A s.t. λ_A=H(μ_A)

1. Chooses μ_C

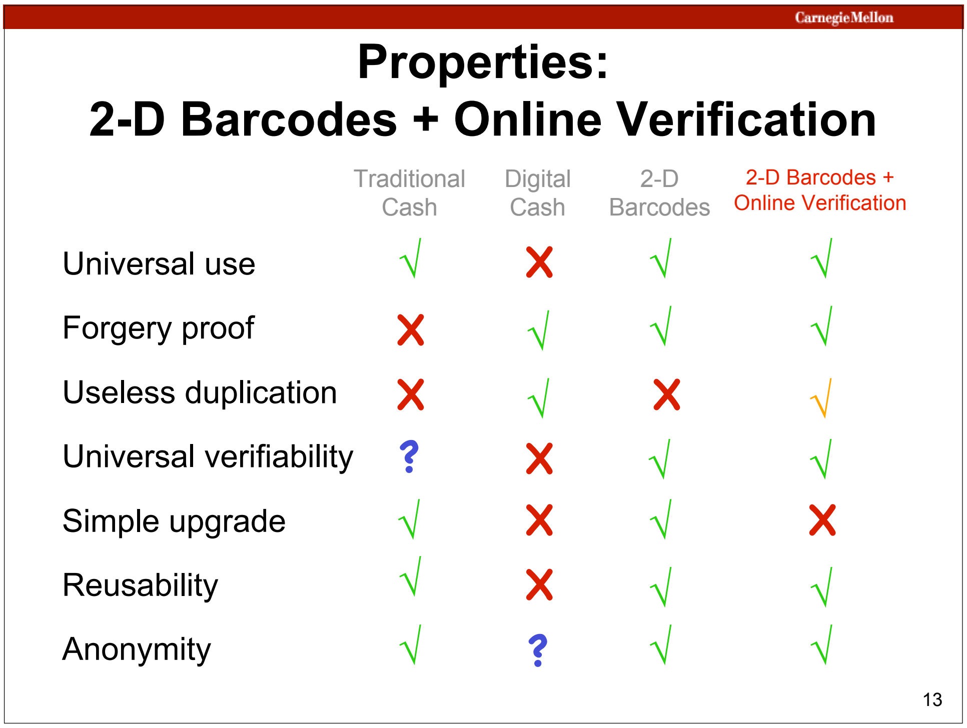
2. Computes λ_C =H(μ_C)

4. $\{N, \mu_A, \lambda_C\}_{E_{Bank}}$

5. Checks λ_A=H(μ_A)

6. $\{N, \lambda_C\}_{S_{Bank}}$

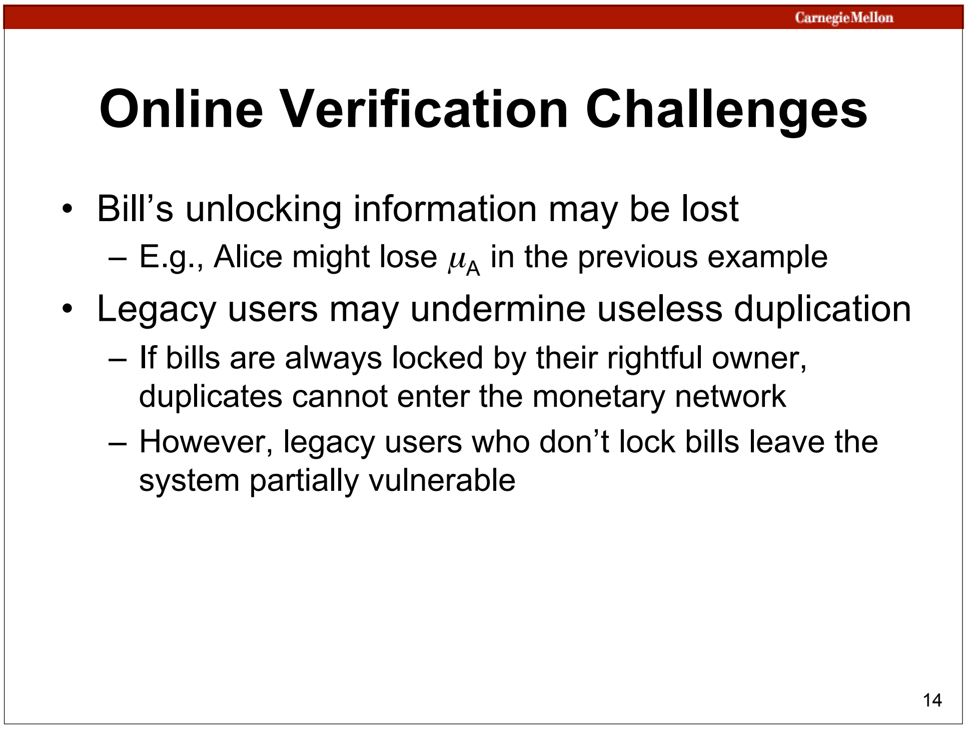
7. $\{N, \lambda_C\}_{S_{Bank}}$



CarnegieMellon

Properties: 2-D Barcodes + Online Verification

	Traditional Cash	Digital Cash	2-D Barcodes	2-D Barcodes + Online Verification
Universal use	√	X	√	√
Forgery proof	X	√	√	√
Useless duplication	X	√	X	√
Universal verifiability	?	X	√	√
Simple upgrade	√	X	√	X
Reusability	√	X	√	√
Anonymity	√	?	√	√



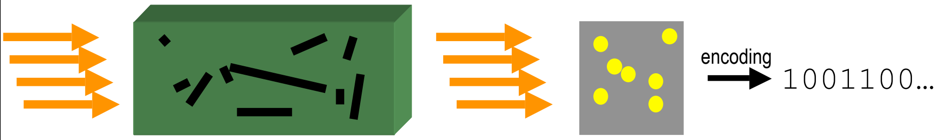
CarnegieMellon

Online Verification Challenges

- Bill’s unlocking information may be lost
  - E.g., Alice might lose μ_A in the previous example
- Legacy users may undermine useless duplication
  - If bills are always locked by their rightful owner, duplicates cannot enter the monetary network
  - However, legacy users who don’t lock bills leave the system partially vulnerable

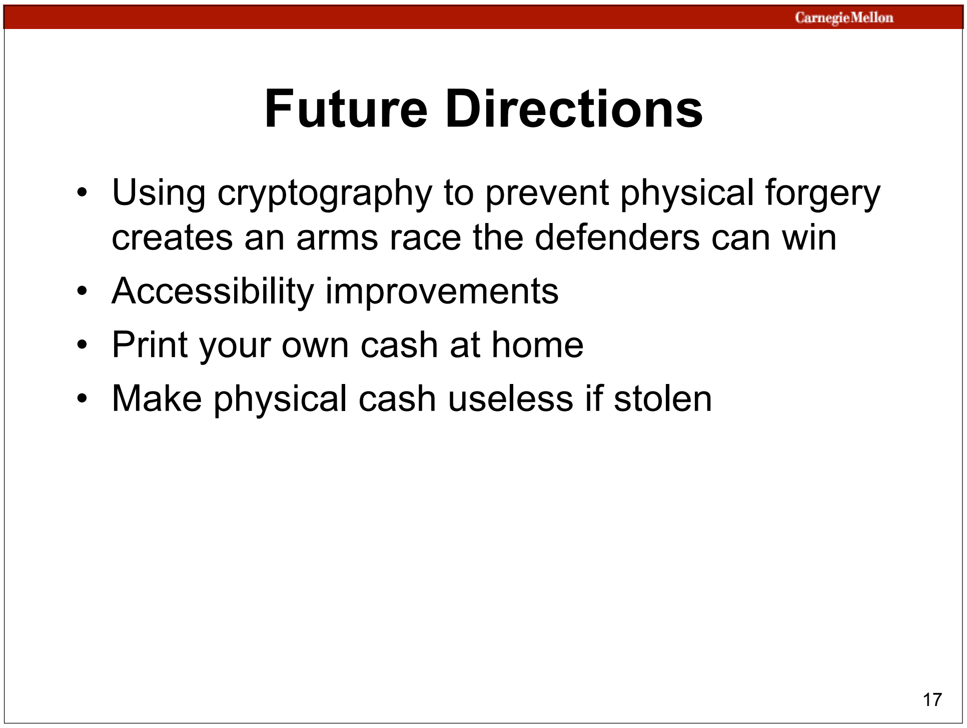
Bank Arbitrage

- If locking information is lost or incorrect…
- Then the bill needs to be returned to the bank, which decides whether the bill is genuine or not
- Drives forgeries back to banks
  - Helps forensics and reduces impact of forgeries
- Bank uses Physical One-Way Functions [Simmons, 1991] [Pappu et al., 2002]
  - Derive unique identifier based on the bill's physical structure



Three-Tier User Hierarchy

Type of user	Examples	Equipment needed	Capabilities
Legacy users	Individuals, some merchants	None	None - can only inspect bills visually
Regular users	Individuals, most merchants	Low-end networked scanning equipment (e.g., cell phone, bill counter)	Can scan and verify bills online
Institutional users	Banks, National Treasury	High-end scanner	Can scan and verify bills, can resolve locking situations

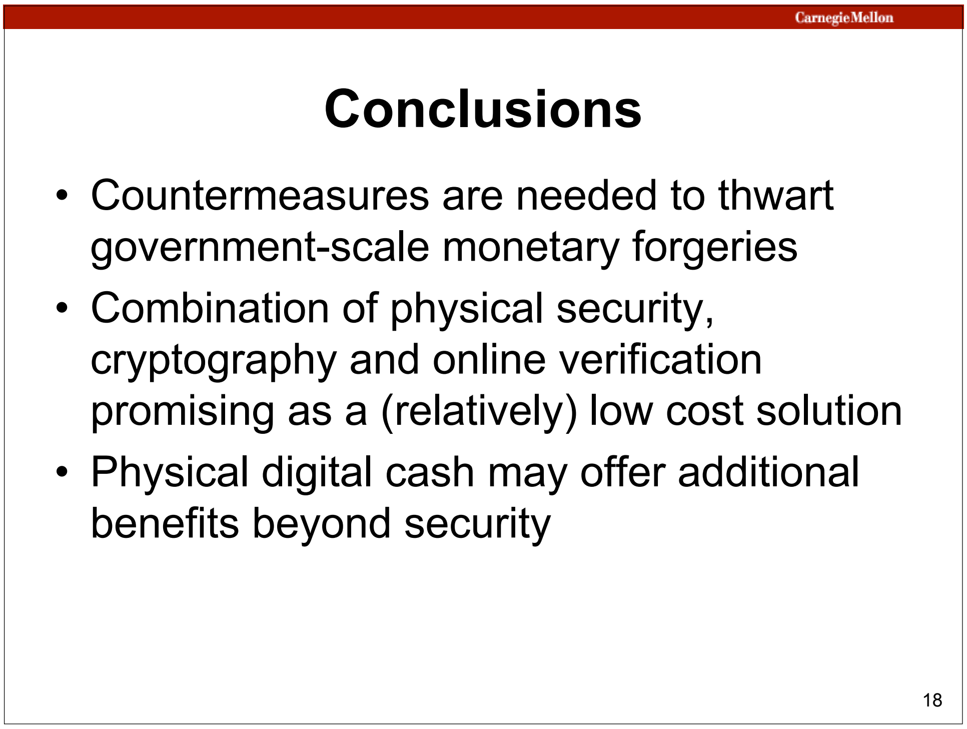


Carnegie Mellon

Future Directions

- Using cryptography to prevent physical forgery creates an arms race the defenders can win
- Accessibility improvements
- Print your own cash at home
- Make physical cash useless if stolen

17

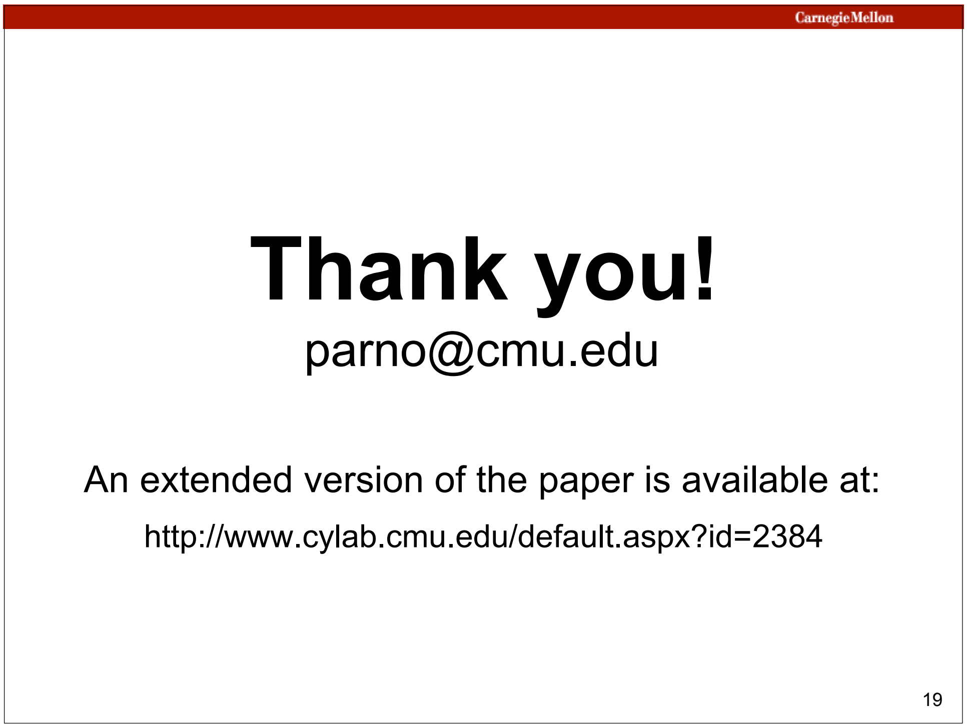


Carnegie Mellon

Conclusions

- Countermeasures are needed to thwart government-scale monetary forgeries
- Combination of physical security, cryptography and online verification promising as a (relatively) low cost solution
- Physical digital cash may offer additional benefits beyond security

18



Thank you!

parno@cmu.edu

An extended version of the paper is available at:

http://www.cylab.cmu.edu/default.aspx?id=2384