user scalability for Bitcoin

Jeremy Clark
Concordia Institute for Information Systems Engineering

Time Stamping

Prediction Markets

Anonymity

Solvency

Usability

History & SoK

Time Stamping

Prediction Markets

Anonymity

Solvency

Usability

History & SoK

Scalability

- Transactions per second
- Maximum block size
- Unspent transaction outputs pool size
- Network propagation
- Orphan rate

User Scalability

- Incentives to use Bitcoin
- Usability
- Risk: price volatility, legality, assurances

Why use Bitcoin?

Why use Bitcoin?

Bitcoin: Economics, Technology, and Governance

R Böhme (U Innsbruck), N Christin (CMU), B Edelman (Harvard), T Moore (U Tulsa)

***Journal of Economic Perspectives*, 29(2): 213-38**

$100

Customer	Merchant	Cost
Credit Card	USD	

Customer	Merchant	Cost
Credit Card	USD	

Initial Cost: $100
Cash back from card: 2%
Effective Cost: $98

Customer	Merchant	Cost
Credit Card	USD	$98

Initial Cost: $100
Cash back from card: 2%
Effective Cost: $98

Customer	Merchant	Cost
Credit Card	USD	$98
BTC	BTC	

Customer	Merchant	Cost
Credit Card	USD	$98
BTC	BTC	

Initial Cost: $100
Merchant saves 3% fee
Bitcoin miner fee: negligible
Effective Cost: $97

Customer	Merchant	Cost
Credit Card	USD	$98
BTC	BTC	$97

Initial Cost: $100
Merchant saves 3% fee
Bitcoin miner fee: negligible
Effective Cost: $97

Customer	Merchant	Cost
Credit Card	USD	$98
BTC	BTC	$97

Realistic?

Customer	Merchant	Cost
Credit Card	USD	$98
BTC	BTC	$97
USD	BTC	

Customer	Merchant	Cost
Credit Card	USD	$98
BTC	BTC	$97
USD	BTC	

Initial Cost: $97
Bank deposit fee: $20 flat (for <$1K) = 2%
Currency exchange fee: 1%
Effective Cost: $100

Customer	Merchant	Cost
Credit Card	USD	$98
BTC	BTC	$97
USD	BTC	$100

Initial Cost: $97
Bank deposit fee: $20 flat (for <$1K) = 2%
Currency exchange fee: 1%
Effective Cost: $100

Customer	Merchant	Cost
Credit Card	USD	$98
BTC	BTC	$97
USD	BTC	$100
BTC	USD	

Customer	Merchant	Cost
Credit Card	USD	$98
BTC	BTC	$97
USD	BTC	$100
BTC	USD	

Initial Cost: $97
Currency exchange fee: 1%
Effective Cost: $98

Customer	Merchant	Cost
Credit Card	USD	$98
BTC	BTC	$97
USD	BTC	$100
BTC	USD	$98

Initial Cost: $97
Currency exchange fee: 1%
Effective Cost: $98

Customer	Merchant	Cost
Credit Card	USD	$98
BTC	BTC	$97
USD	BTC	$100
BTC	USD	$98
USD	USD	

Customer	Merchant	Cost
Credit Card	USD	$98
BTC	BTC	$97
USD	BTC	$100
BTC	USD	$98
USD	USD	

Initial Cost: $98 ($100 minus 3% plus 1%)
User fees: 3% (2% plus 1%)
Effective Cost: $101

Customer	Merchant	Cost
Credit Card	USD	$98
BTC	BTC	$97
USD	BTC	$100
BTC	USD	$98
USD	USD	$101

Initial Cost: $98 ($100 minus 3% plus 1%)
User fees: 3% (2% plus 1%)
Effective Cost: $101

Customer	Merchant	Cost
Credit Card	USD	$98
BTC	BTC	$97
USD	BTC	$100
BTC	USD	$98
USD	USD	$101

Takeaway: not that Bitcoin is necessarily worst than CCs (approximation, fees change, etc)

Takeaway: the best scenario is when customers/merchants want to hold BTC

Aside: Remittances

- Best case scenario for Bitcoin: large amounts, timely delivery, cross borders
- Western Union : ~8%
- USD -> BTC : 3%
- BTC -> Peso (Philippines) : ???

western union near Manila, NCR,

Western Union
Money Transfer Service · Rizal Ave

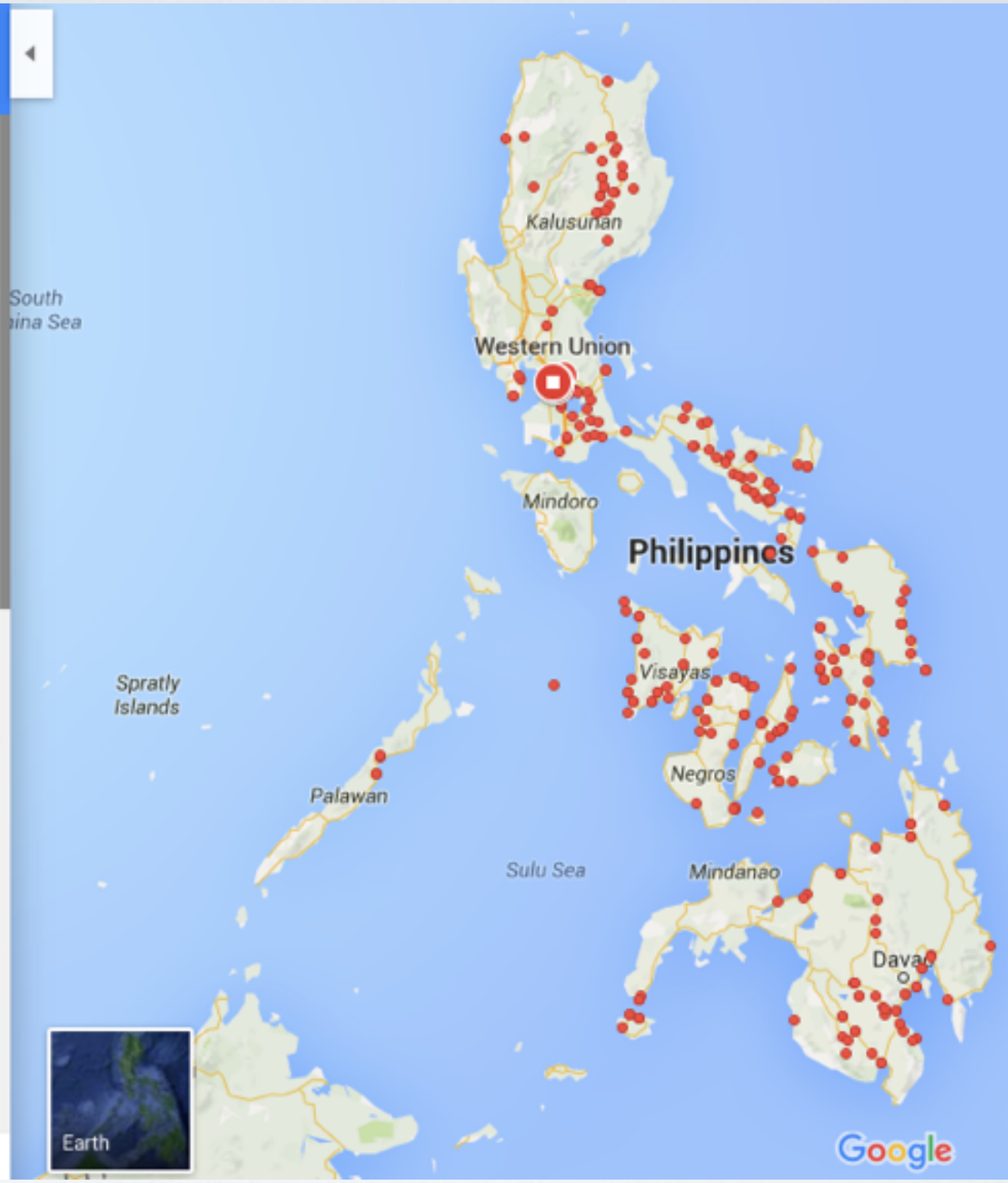
Western Union eBusiness Services Incorporated
CourierLevel 1, Padre Faura Wing, Robinsons ServicePlace Manila, Padre Faura Street, infront of Designers Bloom Store

Western Union
Money Transfer Service · #300 San Diego Street corner, G Tuazon

Western Union
Transfer Service - Money · Gen. Luna St

Western Union
Pawn Shop · Villalobos Street

Showing results 1 - 10



Aside: Remittances

- Best case scenario for Bitcoin: large amounts, timely delivery, cross borders

- Western Union : ~8%

- USD -> BTC : 3%

- BTC -> Peso (Philippines) : ???

- BTC -> Peso via ATMs : 6%

Aside: Remittances

- Best case scenario for Bitcoin: large amounts, timely delivery, cross borders
- Western Union : ~8%
- USD -> BTC : 3%
- BTC -> Peso (Philippines) : ???
- Use BTC instead of converting it

Actually Using Bitcoin

- How do we move from using Bitcoin as a conversion currency to an actual currency?

- We need entities to become legally obligated to use BTC: taxes, salaries, loans, contracts…

- Once some entities are obligated, there will be some permanent demand which creates stability

Usability Issues

Usability Issues

Joint work with:

S. Eskandari (Concordia); D Barrera (ETH Zurich); E Stobert (Carleton)

Classes of Usability Issues

- UI Issues: no barrier to change
- Metaphors & abstractions: moderate barrier
- Foundational: can’t change

UI

- See our paper for a deep dive into performing core tasks with several tools
- Lots of issues: users are not well-guided, it can be hard to determine if a task is complete, lots of jargon

UI

- See our paper for a deep dive into performing core tasks with several tools

- Lots of issues: users are not well-guided, it can be hard to determine if a task is complete, lots of jargon

- “no free outputs to spend”

Metaphors

- Coin
- Wallet
- Address
- Balance

Internet Properties

Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings

☑ Use automatic configuration script

Address: 618 west bethel street

Proxy server

☐ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: [redacted] Port: 80 Advanced

☐ Bypass proxy server for local addresses

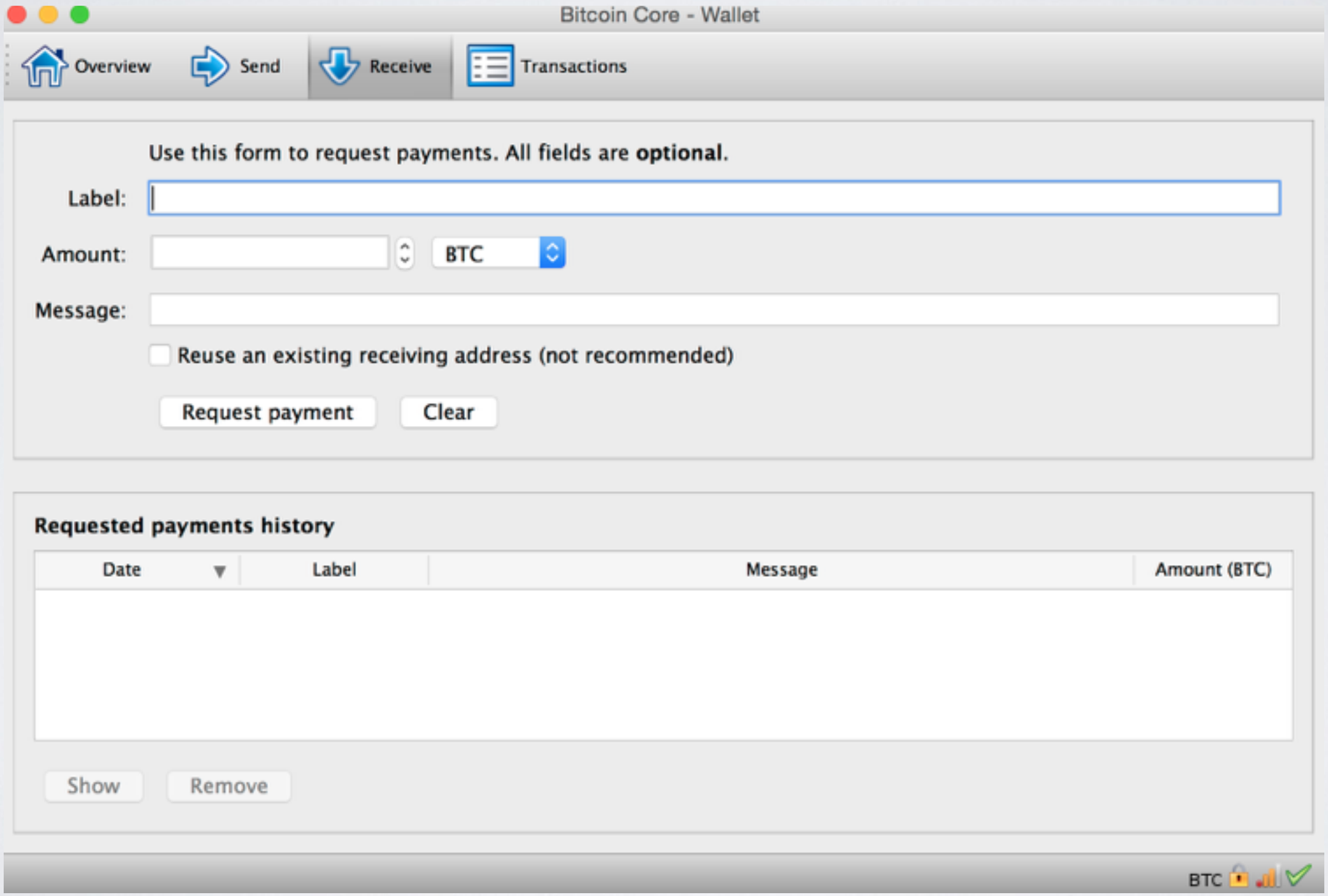
Foundational

- You probably do not use any other technology that relies on cryptographic keys as a user (maybe PGP or SSH)
- The average user does not
- Keys are something you have: subject to loss and theft
- Passwords can be reset if lost
- Password theft is still an issue but banking passwords sell for pennies on the dollar because of other bank procedures to limit theft

Key Management

- How do Bitcoin millionaires sleep at night?
- Best evidence that this is a problem is the variety of approaches
- Store in a file, password protect, password-derive, store offline, paper wallets, hardware security modules, air gapped wallets, online hosted wallets…

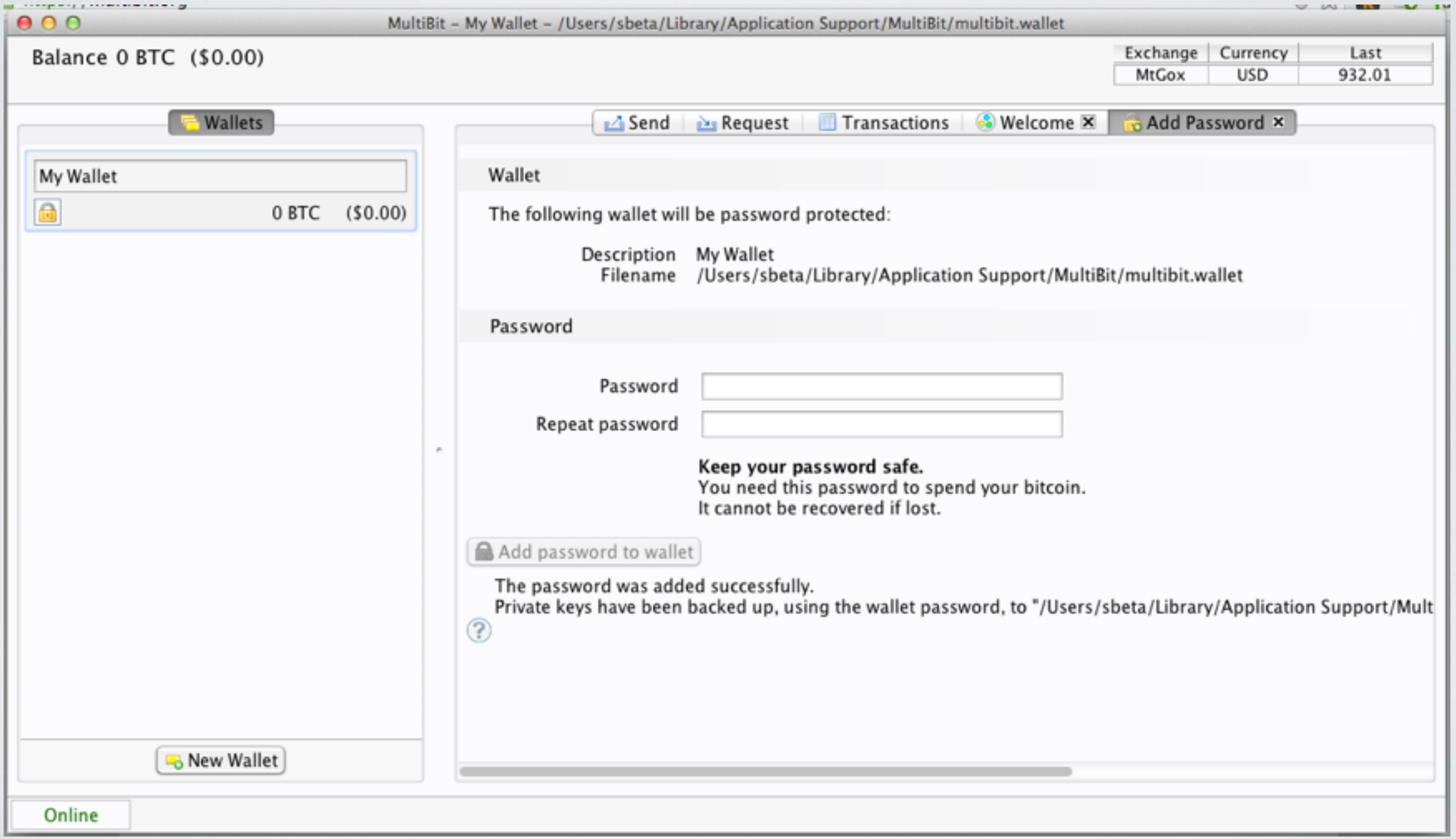
Store in a File



Store in a File

- The idea that keys exist is abstracted away (export/import new functionality)
- portability
- loss/sharing/theft of wallet.dat
- key set in wallet.dat is dynamic (key churn)

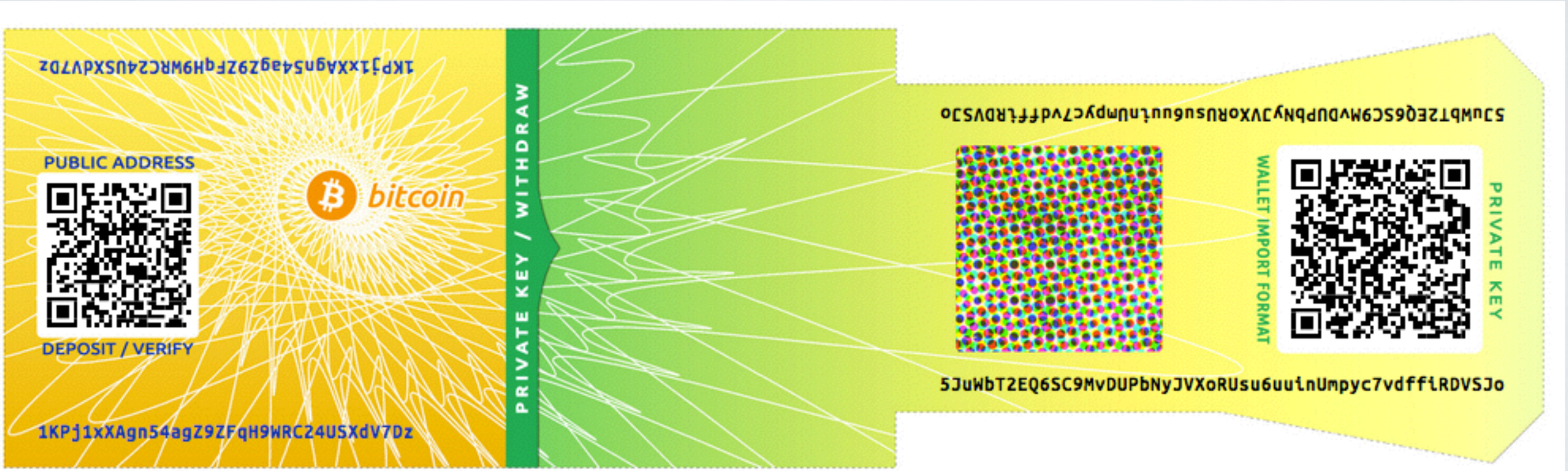
Password-Protected File



Password-Protected File

- Adds a level of protection against theft
- Does not add much against malware (anything password-based: use it while infected, lose it)
- May create wrong mental model where users think of {address, password} as {username, password} -> surprised when using new device

Paper Wallets



Paper Wallets

- You can’t give them away like cash, they can’t be debited like a gift card
- Don’t carry it around in plain site
- Can it be decoded in five years?
- Import it to use: all issues with wallet software apply
- Don’t lose your change


12 days of bitcoin
Bloomberg


BITCOIN
12 days of bitcoin
Bloomberg

Paper Wallets

- You can’t give them away like cash, they can’t be debited like a gift card
- Don’t carry it around in plain site
- Can it be decoded in five years?
- Import it to use: all issues with wallet software apply
- Don’t lose your change

small size of keys. Third, the Bitcoin software can automatically generate keys and create transactions without additional input or actions from the user.

Storing keys locally also creates several threats, which the user must consider. For example, the file storing private keys can be read by any application with access to the user's application folder. Malware authors may be particularly interested in exploiting this key management approach, since access to the local file results in the adversary gaining immediate access to the victim's funds. One of the first examples of private key-stealing malware was discovered by Symantec in 2011 [28], with many other similar malware examples following suit.

Users must be cautious to not inadvertently share their Bitcoin application folder (*e.g.,* through peer-to-peer file sharing networks, off-site backups or on a shared network drive). Physical theft, especially in the case of portable computers or smartphones must also be considered. Similar to the storage of other sensitive files, threats to digital preservation [2] should be taken into account. Examples include general equipment failure due to natural disasters and electrical failures; acts of

Fig. 1. Bitcoin paper wallet generated using https://bitcoinpaperwallet.com. The printout is designed to be folded such that the private key (right) remains hidden while the public component (left) remains visible.

as would be congruent with a traditional mental model for web-based online banking. Users may be surprised to discover that they cannot access their funds at a new device by simply entering their encryption password; the wallet file must also be transferred to the new device.

C. Offline Storage of Keys

small size of keys. Third, the Bitcoin software can automatically generate keys and create transactions without additional input or actions from the user.

Storing keys locally also creates several threats, which the user must consider. For example, the file storing private keys can be read by any application with access to the user's application folder. Malware authors may be particularly interested in exploiting this key management approach, since access to the local file results in the adversary gaining immediate access to the victim's funds. One of the first examples of private key-stealing malware was discovered by Symantec in 2011 [28], with many other similar malware examples following suit.

Users must be cautious to not inadvertently share their Bitcoin application folder (*e.g.*, through peer-to-peer file sharing networks, off-site backups or on a shared network drive). Physical theft, especially in the case of portable computers or smartphones must also be considered. Similar to the storage of other sensitive files, threats to digital preservation [2] should be taken into account. Examples include general equipment failure due to natural disasters and electrical failures; acts of

Fig. 1. Bitcoin paper wallet generated using https://bitcoinpaperwallet.com. The printout is designed to be folded such that the private key (right) remains hidden while the public component (left) remains visible.

as would be congruent with a traditional mental model for web-based online banking. Users may be surprised to discover that they cannot access their funds at a new device by simply entering their encryption password; the wallet file must also be transferred to the new device.

C. Offline Storage of Keys

Paper was peer-reviewed, published, presented, on r/bitcoin, …
Took almost a year for someone to take what we left in this paper wallet

Password-Derived Wallets

- What if you use a password as a seed for generating all the keys you need?

- Great for portability

- Issue is when users choose normal (i.e., bad) passwords -> exhaustive search, rainbow tables, etc

Online Wallets

- Trust a third party!
- However you get an experience much like online banking
- No downloading the blockchain, there is support, passwords can be reset, velocity limits, etc

Category	*Example*	Malware Resistant	Key(s) Kept Offline	No Trusted Third Party	Resistant to Physical Theft	Resistant to Physical Observation	Resilient to Password Loss	Resilient to Key Churn	Immediate Access to Funds	No New User Software	Cross-device Portability
Keys in Local Storage	Bitcoin Core			●		●	●	●	●		
Password-protected Wallets	MultiBit		○	●	○	●		●	●		
Offline Storage	Bitaddress	○	●	●			●				●
Air-gapped Storage	Armory	○	●	●		●	●	●			
Password-derived Keys	Brainwallet		●	●	○			●	●	●	●
Hosted Wallet (Hot)	`Coinbase.com`						●	●	●	●	●
Hosted Wallet (Cold)		○	●				●	●		●	●
Hosted Wallet (Hybrid)	Blockchain.info		○	○			●	●	●	●	●
Cash		●	●	●		●	●	●	●	●	●
Online Banking							●	●	●	●	●

TABLE I. A COMPARISON OF KEY MANAGEMENT TECHNIQUES FOR BITCOIN (CONTRASTED WITH TRADITIONAL FINANCIAL SERVICES). ● INDICATES THE CATEGORY OF CLIENT IS AWARDED THE BENEFIT IN THE CORRESPONDING COLUMN. ○ PARTIALLY AWARDS THE BENEFIT. DETAILS PROVIDED INLINE.

Takeaway 1: nothing comes close to cash

Takeaway 2: on usability alone (not security), online wallets are the best

Hosted Wallet Manifesto

- Security people hate hosted wallets
- They are arguably against the Bitcoin's principals
- BUT they offer the best shot at user scalability
- Idea: stop shaming people for using online wallets or keeping their BTC on exchanges
- Instead work at making these as secure as possible
- Not a bad compromise: trust agility

Risk Issues

Risk Issues

- Price volatility -> need models and futures
- Legality and tax status -> will come in time
- Third party risk -> fraudulent/incompetent exchange services and hosted wallets

e.g., Mt Gox's missing $450M

Third Party Risk

- Bitcoin companies are generally newer than Bitcoin itself: short reputation
- Bitcoin companies are generally not diversified, so some lost on the Bitcoin side means bankruptcy
- User scalability: imagine legacy companies (e.g., banks) offer insured exchange and hosted wallet services
- Stop-gap solution: cryptographic proof of solvency

Solvency Proofs

Joint work with:

G. Dagher (Concordia); B Bunz, J Bonneau, D Boneh (Stanford)

Solvency Proofs

- Solvency proofs are easy if you don't care about privacy: (i) publish a list of your customers and balances (liabilities); (ii) publish a list of your bitcoin addresses (assets) and demonstrate control over them

-----BEGIN PGP SIGNED MESSAGE-----

On Monday February 24th, 2014 I was invited to the offices of Coinbase in San Francisco... My goal during this visit was to validate the existence and security of customer funds.

While Coinbase publicly states that up to 97% of customer funds are in cold storage, at the time of my visit, their internal reporting tool showed that the cold storage system contained 98.8% of customer funds. To confirm for myself that these funds were in the cold storage system, I looked up the balance each of the cold storage addresses against the public blockchain, using an external site...

...I randomly selected one of the cold storage addresses and requested that a transaction be signed to prove ownership of the address.

Based on what I observed during my visit and my experience in security, it appears that the Coinbase system contains the expected funds and their cold storage system and process appear to be operating according to security best practices.

Andreas M. Antonopoulos

-----BEGIN PGP SIGNATURE-----

Provisions (in one slide)

- Privacy preserving solvency proofs: throw lots of crypto at the problem
    - Publish individual account records that can be individually verified
    - Sum up these records homomorphically
- Harvest every {address (full key), balance} from the blockchain
    - a zero knowledge proof that you know the private keys of some subset of these
    - Sum up their balances
- Prove in zero knowledge: sum of assets >= sum of liabilities

Future Work

- Usability of transacting with Bitcoin
- Usability of exchanging fiat to/from Bitcoin
- User *studies*: we only did a cognitive walkthrough
- Security solutions for hosted wallets that do not sacrifice the usability benefits
- Proof of solvency: full end-to-end implementation

Future Work

- Usability of transacting with Bitcoin
- Usability of exchanging fiat to/from Bitcoin
- User *studies*: we only did a cognitive walkthrough
- Security solutions for hosted wallets that do not sacrifice the usability benefits
- Proof of solvency: full end-to-end implementation
- Blockchain forensics: what is Gavin's salary?

Questions

@PulpSpy

j.clark@concordia.ca