


Welcome!

Institutions and Individuals
Need Effective Decentralized
Privacy Solutions

Super Quick Intro

Title	Organization	
Regulatory Compliance Analyst	DV Chain dvtrading.co/dv-chain	
Organizer	Monero Community Workgroup #monero-community	
Board Member	MAGIC magicgrants.org	
Host and Researcher	Breaking Monero Breaking Zcash	
Publisher	<i>Mastering Monero</i> masteringmonero.com	
Moderator	r/CryptoCurrency reddit.com/r/cryptocurrency	
Former President	Minnesota Cryptocurrency mncryptocurrency.org	








Blockchain
Training
Conference
AUGUST 28-30 | DENVER



MONERO

Quick Definition Quadrant

	Transparent	Obfuscated
Public	 bitcoin  ethereum	 MONERO  Zcash
Private	 HYPERLEDGER Private Bitcoin/Ethereum Instance	Private Monero/Zcash Instance

Note: **obfuscated** is an oversimplification, which I will cover later in this talk

Activity

Name

Activity

Name to Alice



**Blockchain
Training
Conference**
AUGUST 28-30 | DENVER



MONERO

Activity

Name to Alice

Alice to Bob

Activity

Name to Alice

Alice to Bob

Bob to Charlie

Activity

Name to Alice

Alice to Bob ●

Bob to Charlie

Activity Debrief

Who accepted cards with red dots on them? Why?

Who could not send their funds to anyone else?

Would anyone accept the funds at a discount for the trouble?

Who would pay more for a card with no previous history?

Activity Debrief

Transparent blockchains look much like these cards

Sending and
receiving addresses
and amounts are
visible to all

Name to Alice

Alice to Bob

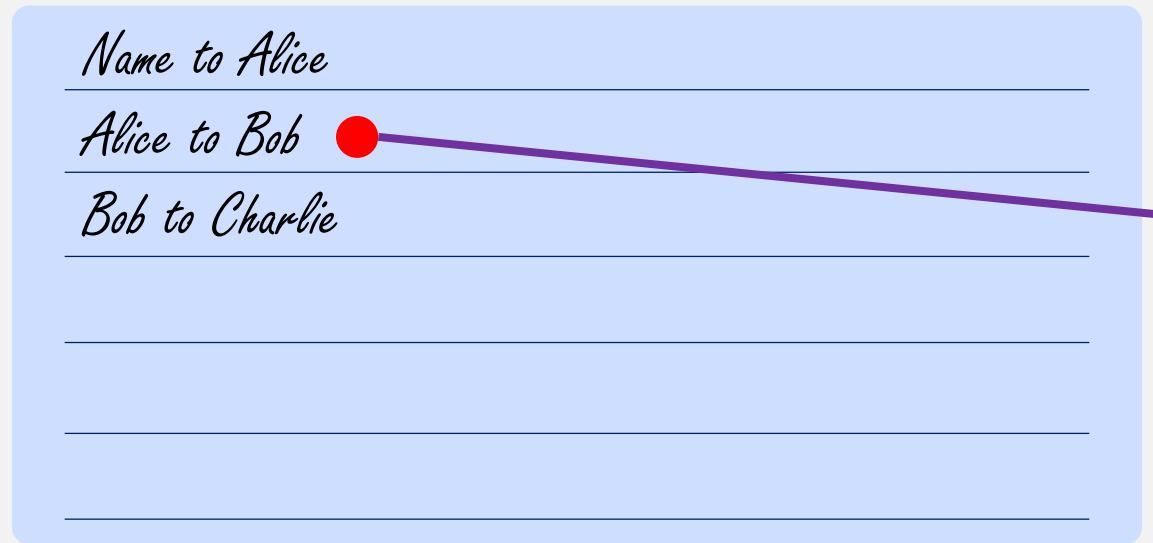
Bob to Charlie

Exchanges collect IDs,
SSNs, addresses, etc.

Blockchain analysis
companies compile lists
of suspicious accounts;
most companies
subscribe to these, but
few users do

Activity Debrief

Transparent blockchains look much like these cards



Bob Profile

Amount: 10 BTC

Suspicious Activity:

Ransomware

Risk profile: **High**

Privacy as Optionality

Name to Alice

Alice to xxxxx ●

xxxxx to Charlie

xxxxx Profile

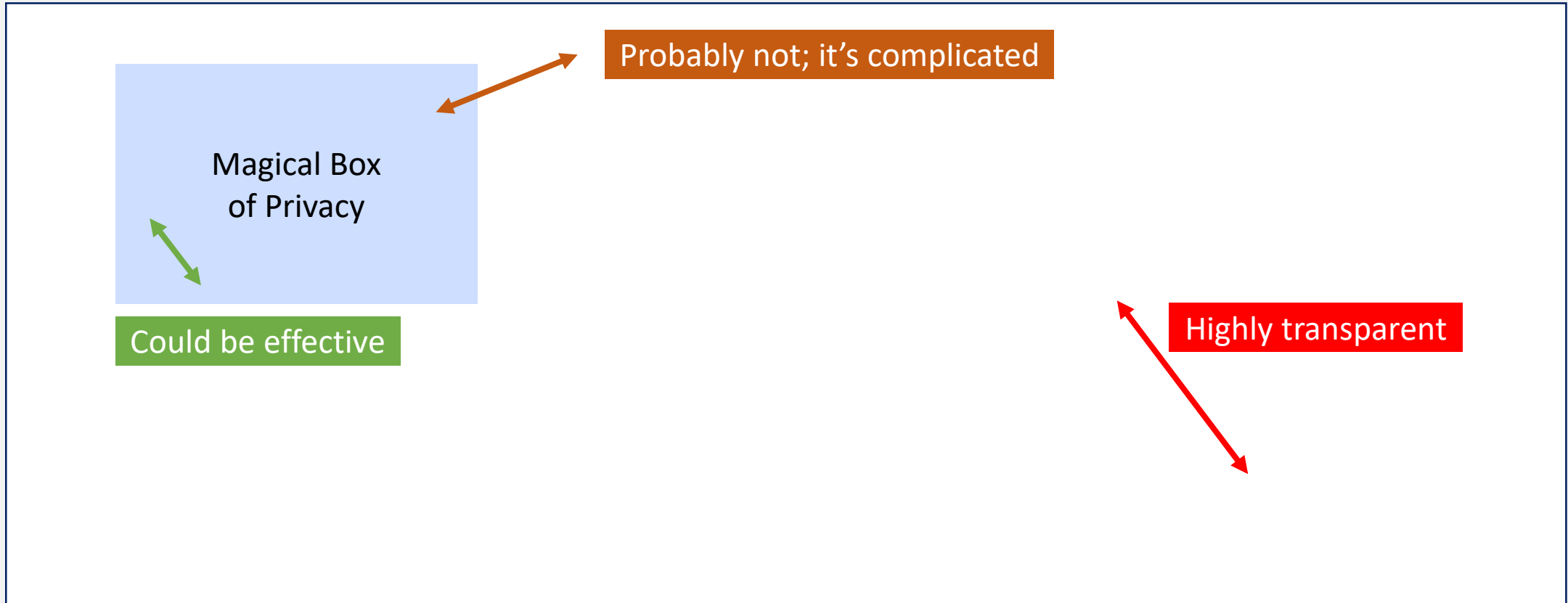
Amount: 10 BTC

Suspicious Activity:

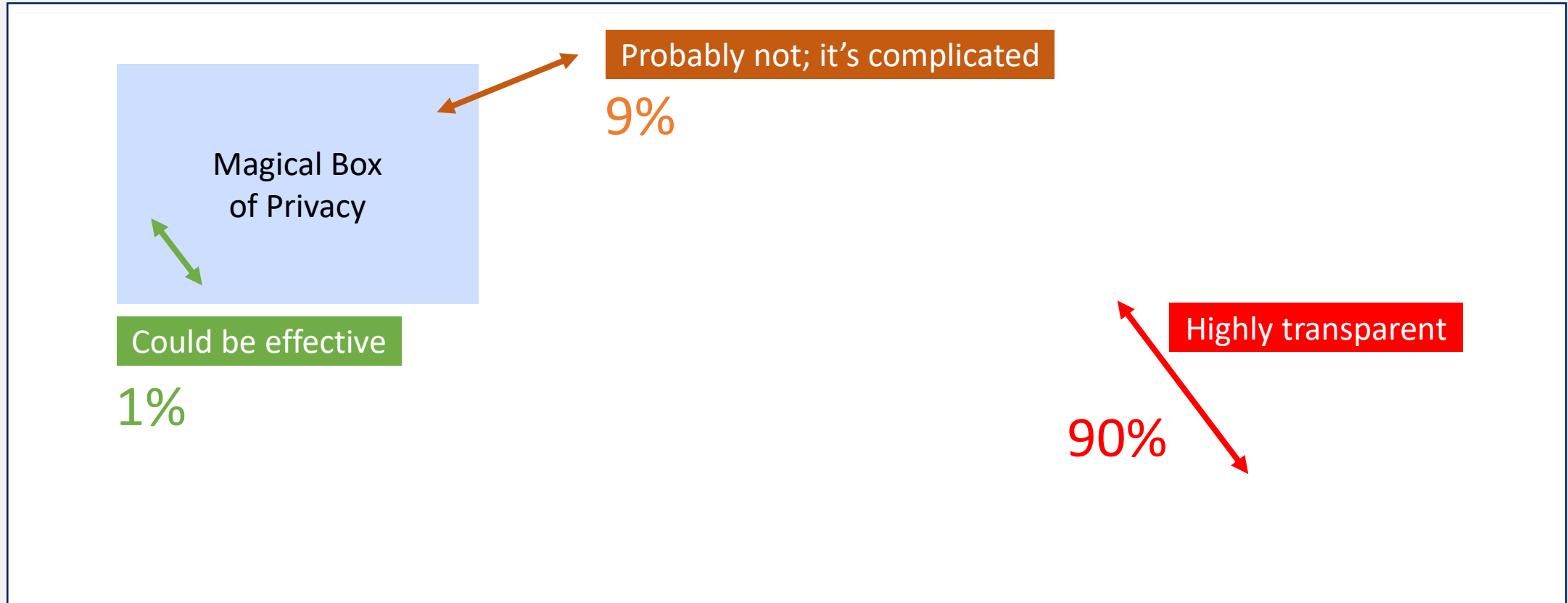
Used Privacy Feature

Risk profile: Medium

Tools Can Be Added; Complicated Benefits



Tools Can Be Added; Complicated Benefits



Privacy Feature Use by Default Function

Opt-In



Opt-Out



Mandatory



Opt-In: Zcash transparent, partially-shielded, and fully-shielded transactions
Opt-Out: Monero ringsize by transaction February 2016

Another Real-Life, Non-Crypto Example



How Does This Impact People, Practically?

Bitcoin Wiki recommends solo mining funds (good luck)

Bitcoin trades at a discount to Monero on decentralized exchanges
High risk of receiving tainted Bitcoin

“Fresh” Bitcoin commands a 5-10% premium

Individuals and businesses are at risk of unintentionally accepting tainted coins in otherwise legal business transactions.

Privacy is Critical for Business

No one (esp. competitors) should see DV's counterparty list

No one should see when we transfer BTC to exchanges

What if someone tries to front-run the trade?

Compliance is simpler if there is no public record of payment history

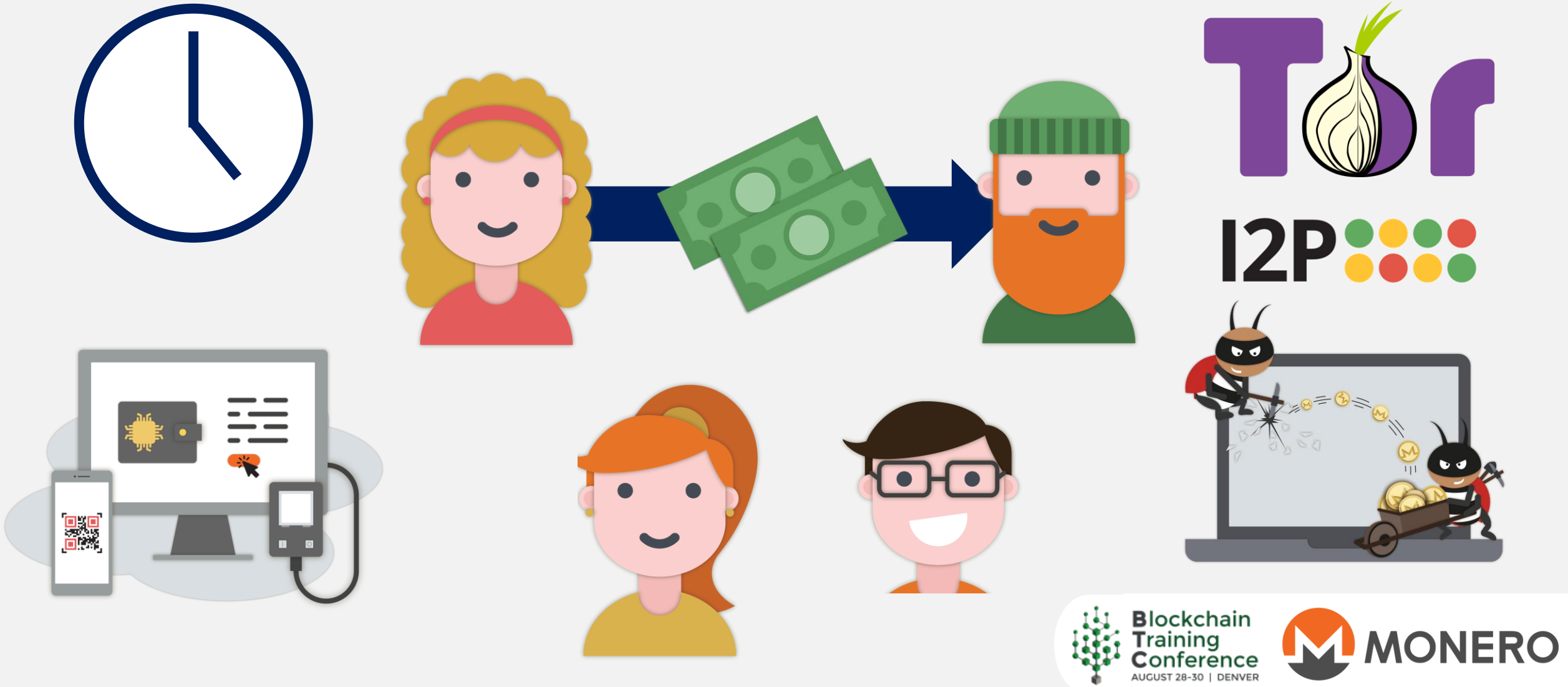
Revert to back-to-basics KYC approach

Who checks the source of funds for a low-risk \$5 cash payment?

The Problem: Privacy is **HARD**



The Problem: Privacy is **HARD**



The Problem: Privacy is **HARD**

Privacy features may be on/off like a light switch, but reality is far more complicated, even for good privacy options.



Zero-Knowledge Isn't Perfect



Zero-Knowledge Isn't Perfect

Zero-knowledge proofs are hot topics and sound amazing

Zero-knowledge proofs address *specific* problems, but they do so with varying levels of success and with different tradeoffs

Patching one hole doesn't mean the other holes are magically patched



Fungibility is the Main Goal

Digital money where 1 BTC \neq 1 BTC *sucks*

Inspecting funds before receiving or sending them *sucks*

Bitcoin is *fungible-ish* for the worst of both worlds:

- Normal people accept it without thinking, assuming it's fungible

- Services audit and close accounts based on linked behavior

- Normal, unsuspecting users at highest risk

- Businesses still suffer from consequences of transparency

Optional privacy wallets are insufficient

Fungibility is the Main Goal

Without fungibility, we've created the same financial system as before

Surveillance companies function as payment processors to audit incoming funds for compliance purposes

Fungible assets avoid this problem



Conclusion

Privacy is very difficult but an essential property

Individuals and businesses need privacy to transact

Privacy nuances are difficult to comprehend; the solution needs to be simple to use

We need to get away from the “efficiency first, privacy second” mindset

Without privacy, open blockchains will be used primarily for surveillance purposes

Questions?

jehrenhofer@dvtrading.co
justin@ehrenhofer.org