

Bitcoin2Go: Secure Offline and Fast Payments with Bitcoins

Alexandra Dmitrienko, David Noack, Ahmad-Reza Sadeghi, and Moti Yung

Motivation

- Bitcoin thrives to be the most successful crypto currency
- Transaction verification in Bitcoin requires online access and time
- Not applicable in offline payment scenarios (e.g., PoS, vending machines, etc.)
- Fast payments with Bitcoins are vulnerable to double spending attacks

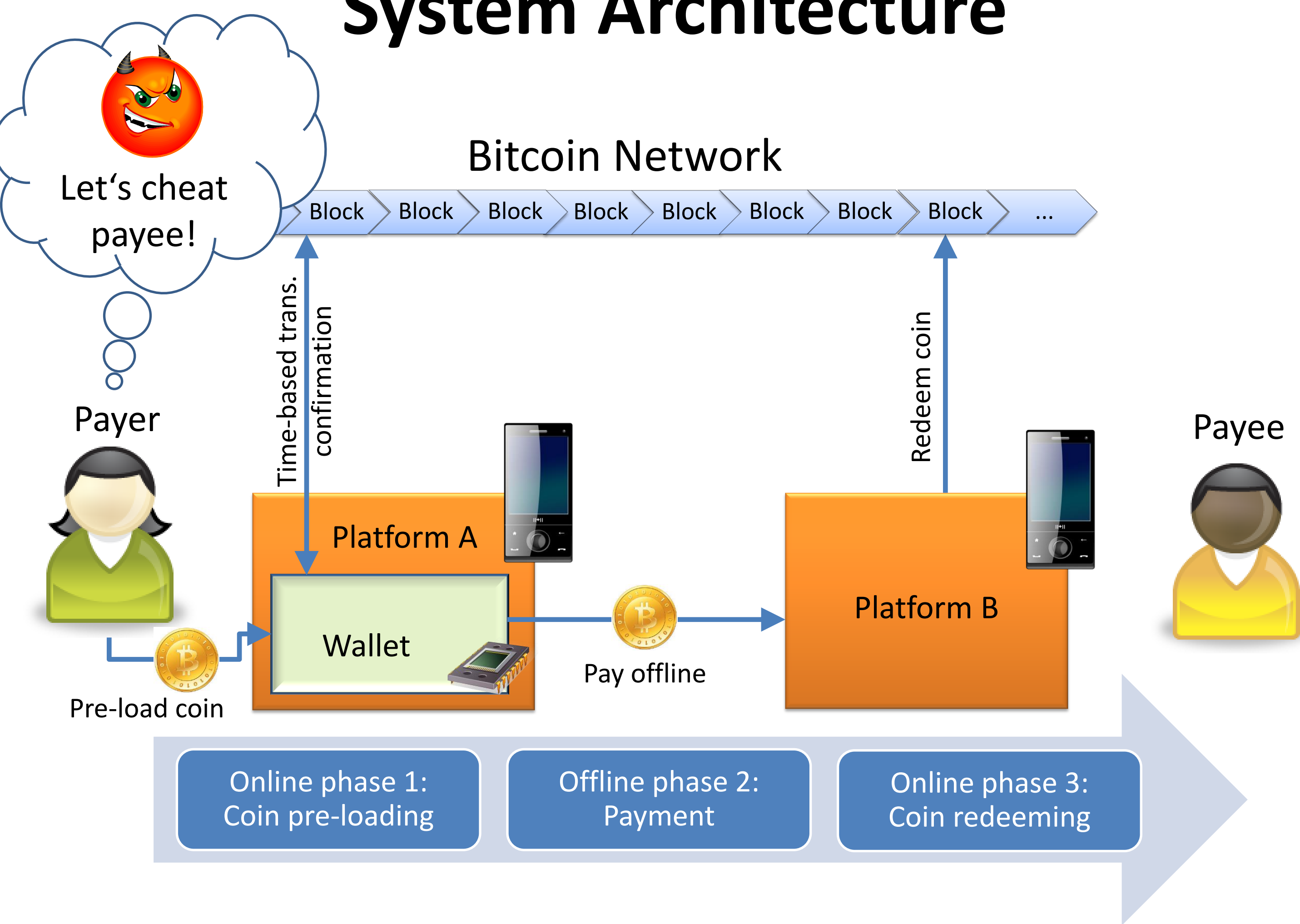
Related Work

- Covers security, privacy and economical aspects of Bitcoin online payments
- No attempts to adapt to offline scenarios

Challenges of Offline Payments

- Double-spending prevention and detection of forged coins in offline settings

System Architecture



Features

- Compatible to Bitcoin system
- Designed for resource constraint wallets
- Can be used by PCs and smartphone-based clients

Security Mechanisms

- Secure, but resource constraint wallet
 - Prevents double spending in offline phase
 - Resource constraints raise challenge to verify pre-loading transactions
- Time-based transaction confirmation
 - Restricts standard Bitcoin transaction confirmation generation by max. time
 - Probability to produce valid confirmation is high for the Bitcoin network, but low for an attacker
- Limited transaction amounts
 - Attack costs become higher than benefits

Prototype Implementation

Host platform:

- Galaxy S3 with Android 4.0.4

Wallet:

- Secure element in microSD card
- JavaCard 2.2.2, JCOP 2.4.1
- 81 Kb EEPROM, 20 Kb code, 1 Kb RAM footprint



Risk Analysis

	Set 1	Set 2	Set 3
Attacker's hashrate, %	10	15	20
Min. length of the trans. conf., blocks	6	7	10
Max. time for generation of a single block, sec.	1000	1200	1200
Attack probability, %	1	1	1
Attack costs per block, EUR	560	560	560