Thing-to-Thing Electricity Micro-Payments Using Blockchain Technology

Thomas Lundqvist, Andreas de Blanche, H. Robert H. Andersson Department of Engineering Science University West, Trollhättan, Sweden thomas.lundqvist@hv.se





Thing-to-thing micro-payments



Characteristics:

- Small and numerous
- Autonomous
- Secure
- Private
- Reliable

Plug in cable

- -> Cable or appliance starts paying socket
- -> Socket starts delivering power



Blockchain technology

- Bitcoin, Satoshi Nakamoto, 2008
- Decentralized, open, peer-to-peer network
- No central trust:
 - No single bank or company controls the availability and use
- The blockchain database is a distributed ledger
- Proof-of-work algorithm (mining) makes the blockchain hard to rewrite



Status, June 2017:

1 BTC is \$2500

Trade volume (24h) is 600,000 BTC (95,000 BTC on-chain)



Bitcoin and micro-payments?

Promising technology for thing-to-thing micro-payments:

- No central authority
- Reliable
- Interoperable
- Secure and private
- Easy account creation
 - each thing can have its own account



12,000 nodes June 2017



Purpose of study

Examine the feasibility of using bitcoin in autonomous thing-to-thing payments

Results:

- A proof-of-concept prototype system
- A new single-fee micro-payment protocol
- Limitations and possible pitfalls



Proof-of-concept system



We built a smart cable that connects to a smart socket The smart cable pays the socket using Bitcoins for electricity





Proof of concept

We toasted one slice of bread:

- 1300 W toaster
- 40 Wh of energy
- 5 payment transactions

Total cost: 5 x 0.1 mBTC + bitcoin fees



Bitcoin transactions



ECDSA: Elliptic Curve Digital Signature Algorithm Offline account generation: public and private key



One of the bitcoin transactions

17426e6f9d4925029eb52e87d97c9598a6b5bc04d6ebaf23e34af990ef7e3b06		mined Feb 9, 2017 4:10:52 AM	
1AQuzcmm9XimkVeGFfK7s1hHCYy7VffW7U 0.5035 mBTC	>	1LkE18xg6ZMA82rBqeycc3K26KntdWmdDF	0.1 mBTC (U)
		1AQuzcmm9XimkVeGFfK7s1hHCYy7VffW7U	0.2775 mBTC (S)
FEE: 0.126 MBTC		17840 CONFIRMATIO	ONS 0.3775 MBTC





The new single-fee micropayment protocol



Trust considerations

Trust issues:

- Cable tries to fool socket
- Socket tries to fool cable

Solutions:

- Payments should be small
- Cable must check transaction carefully before signing
- Socket must check transaction carefully before broadcasting



Conclusions

Micro payments using blockchain technology are feasible

The bitcoin blockchain has limitations:

- Too high relative fee for transactions
- Limited transaction capacity

Further obstacles:

- Account handling needs to be more user friendly
- Accounts must not be lost when things break



Questions?



Technical considerations

From prototype to production:

- Boot time should be faster: 27 sec to first payment in prototype
- Reliance on third-party API:
 - Full node: 120 GB storage (June 2017)
 - SPV-node: 35 MB storage (June 2017)
- Enough processing power is needed for crypto operations



System states



