Bernd Petak
Consulting

Understanding Bitcoin

...The Two Simple Ideas behind Crypto-Technology.

Bernd Petak - bernd.petak@gmail.com
Twitter - @berndpetak

Disclaimer Statement

I am not an advocate for any cause, trend or technology, but am an avid observer and analyst.

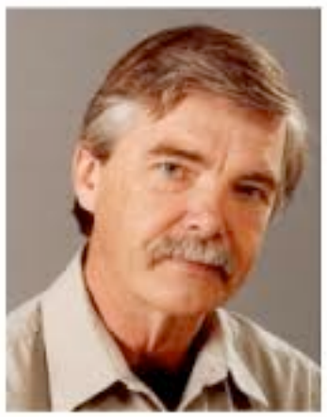
Agenda

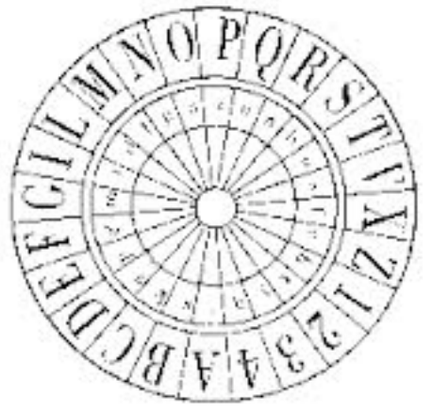
- A brief introduction
- Idea #1 - Public Key Cryptography
- Idea #2 - The Blockchain
- Crypto-Tech Myths and Facts (Busted).

Please help me to refine this presentation to make it better

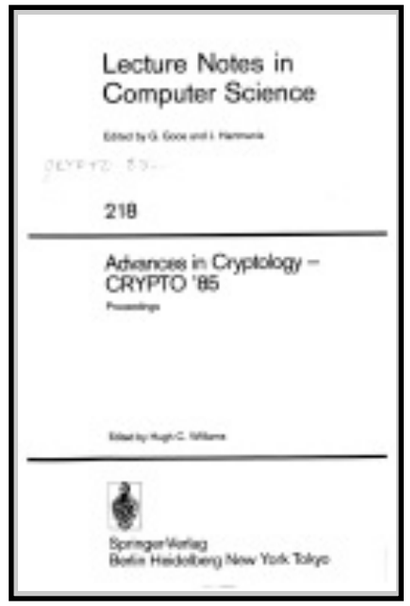
Acknowledgements

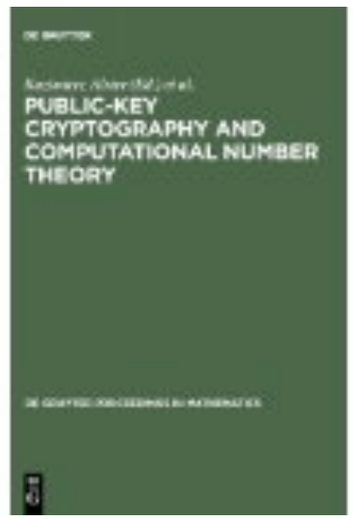
- At my undergrad school our professors had a bizarre research interest.





Cryptography





What a useless way for profs to get research and publishing credits. This stuff has no practical value outside of Ian Fleming novels.

Fast Forward to 2008

- “Satoshi Nakamoto” writes a paper

From: Satoshi Nakamoto <satoshi <at> vistomail.com>
Subject: **Bitcoin P2P e-cash paper**
Newsgroups: **gmane.comp.encryption.general**
Date: 2008-10-31 18:10:00 GMT (4 years, 52 weeks, 1 day, 3 hours and 23 minutes ago)

I've been working on a new electronic cash system that's fully
peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
 Double-spending is prevented with a peer-to-peer network.
 No mint or other trusted parties.
 Participants can be anonymous.
 New coins are made from Hashcash style proof-of-work.
 The proof-of-work for new coin generation also powers the
    network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would
allow online payments to be sent directly from one party to another
without the burdens of going through a financial institution.
Digital signatures provide part of the solution, but the main
benefits are lost if a trusted party is still required to prevent
double-spending. We propose a solution to the double-spending
problem using a peer-to-peer network. The network timestamps
transactions by hashing them into an ongoing chain of hash-based
proof-of-work, forming a record that cannot be changed without
redoing the proof-of-work. The longest chain not only serves as
proof of the sequence of events witnessed, but proof that it came
from the largest pool of CPU power. As long as honest nodes control
the most CPU power on the network, they can generate the longest
chain and outpace any attackers. The network itself requires
minimal structure. Messages are broadcasted on a best effort basis,
and nodes can leave and rejoin the network at will, accepting the
longest proof-of-work chain as proof of what happened while they
were gone.

Satoshi went on to release <u>open source</u> software that fully implements the proposed crypto-currency concept he called “Bitcoin”.

What is Crypto-Technology

- Crypto-technology is a class of computer software systems that can:
  - Implement a system to transfer virtual goods
  - Implement complex agreements between parties
  - Addresses some of the major issues with how these are done currently
  - Do all this using two main ideas

What are Virtual Goods?

- There are many virtual goods that we are already familiar with, including:
    - A **song** on your hard drive.
    - An online **document.**
    - A piece of **software.**
- But there are some virtual goods that might not be obvious:
    - The **“ownership”** of almost anything.
    - An **approval**, **verification** or **notarization** of almost anything.
    - A unit of **currency**

What problems does Crypto address:

Counterfeiting - crypto assures the parties that the original virtual good was transferred, not a copy

Trust of the counter-party is not required to transfer the virtual good; transfers are verified & permanent

Central authority is not required to process transactions or maintain the ledger; no middleman can steal your good

Trust in the network is required. That means that you believe that the majority of "miners" are honest and don't collude.

The Two Main Ideas

- The two main ideas underpinning all crypto-technology are:

Public Key Cryptography

- Assures a virtual good is transferred not copied
- Eliminates need to trust the counter-party

The Blockchain

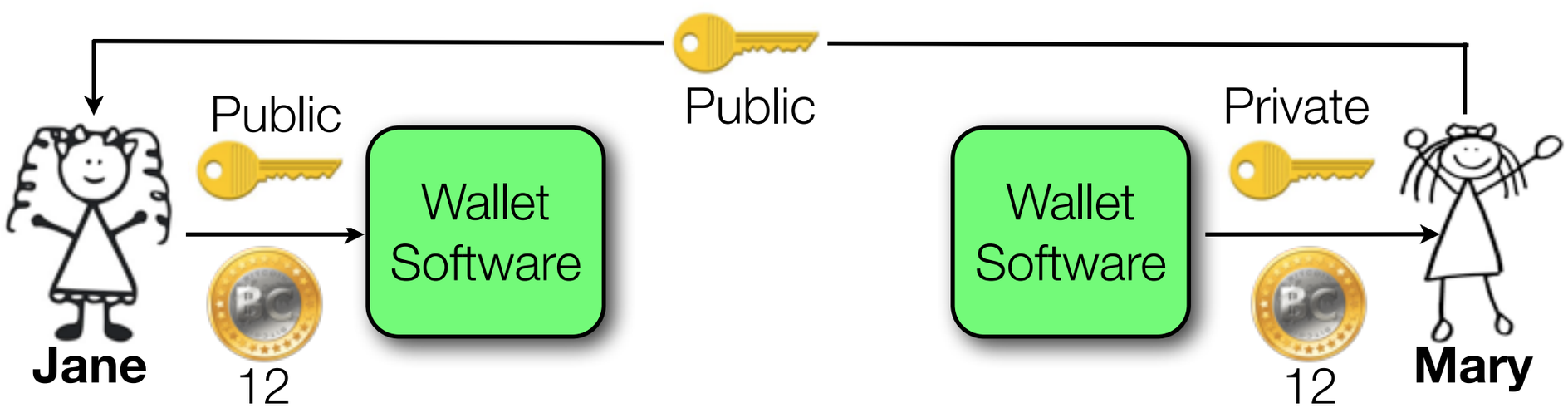
- Eliminates need to trust a central authority
- Makes transfer theft very, very difficult

Idea 1: Public Key Cryptography

- A magical math concept best implemented with computers, that allows an individual to encode a virtual good that can only be decoded by the intended recipient. Once encoded, the even the sender can't decode it.

  - Makes counterfeiting a PKC encoded virtual good very, very expensive

- Uses two big numbers: a private key and a public key



- Solves the double spend problem inherent in electronic transactions.

What is a Ledger?

- A ledger is a two column list of owners and goods. Each line shows a good that the corresponding owner possesses

Before

Owner	Amount
Jane	12
Mary	0
Bob	0

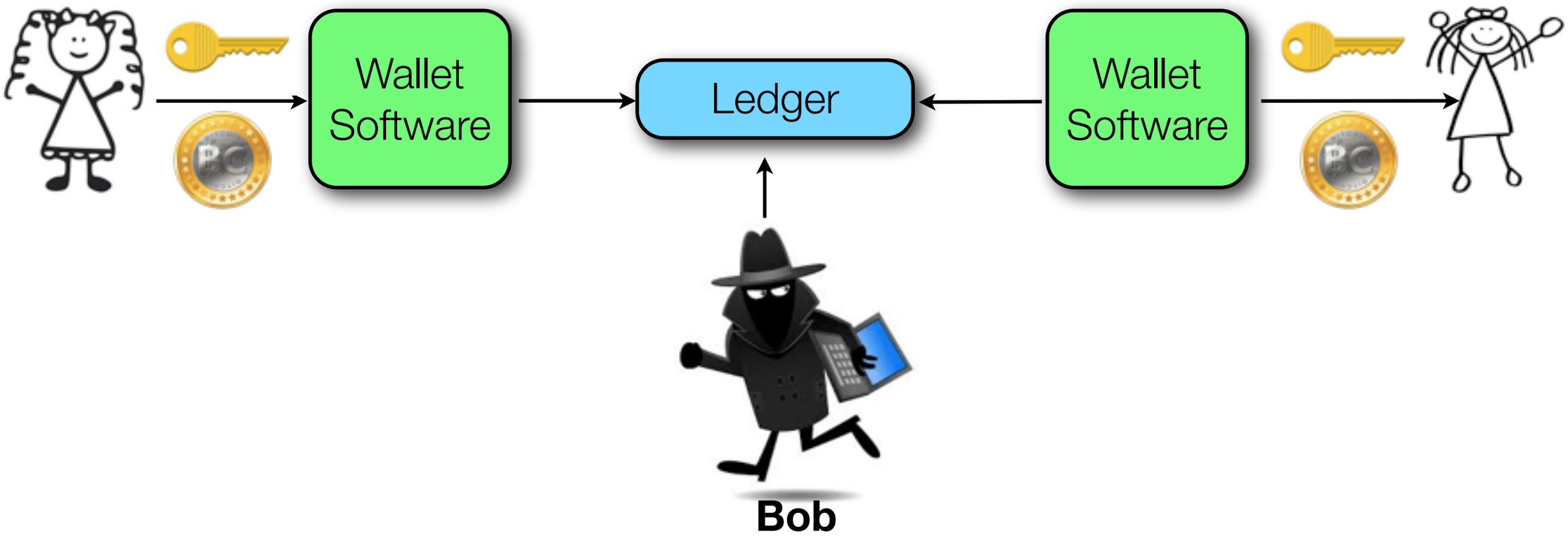
After

Owner	Amount
Jane	0
Mary	12
Bob	0

- The ledger is un-encrypted and visible to all

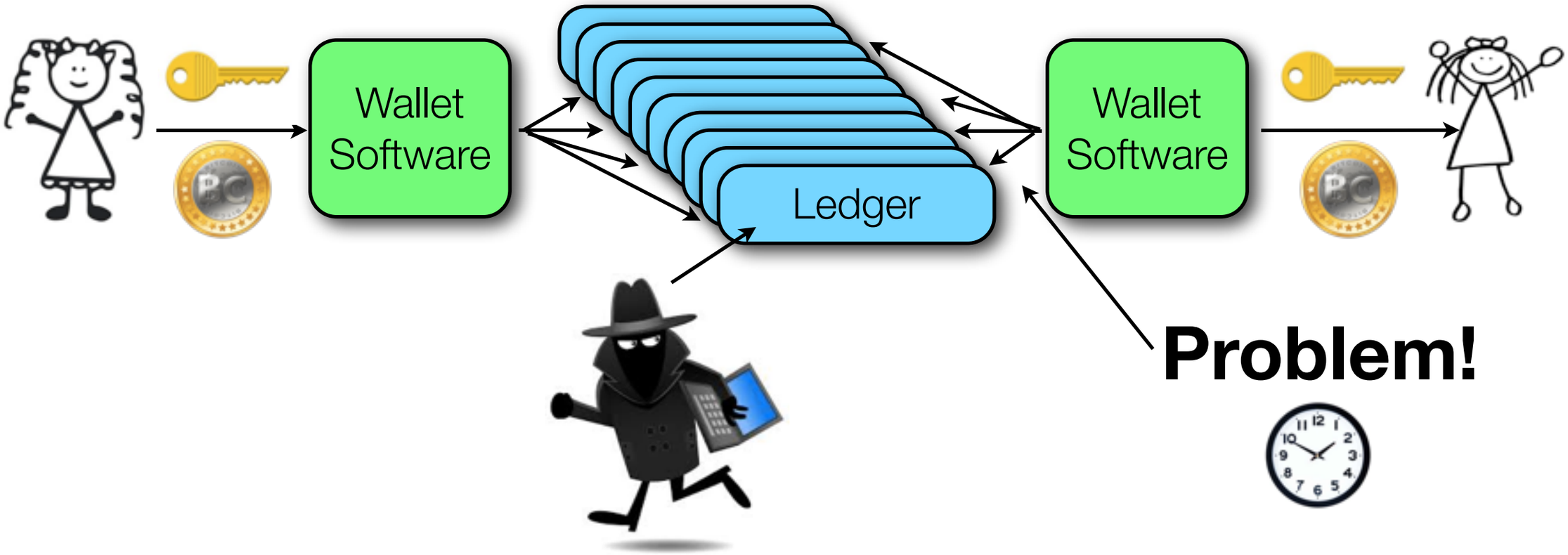
Idea 2: The Blockchain

- A special form of ledger, that keeps track of who holds what, that is very, very hard to fraudulently modify
    - Whenever we want to create a marketplace where people can trade, we need to keep a ledger that “remembers” who owns what.



Idea 2: The Blockchain

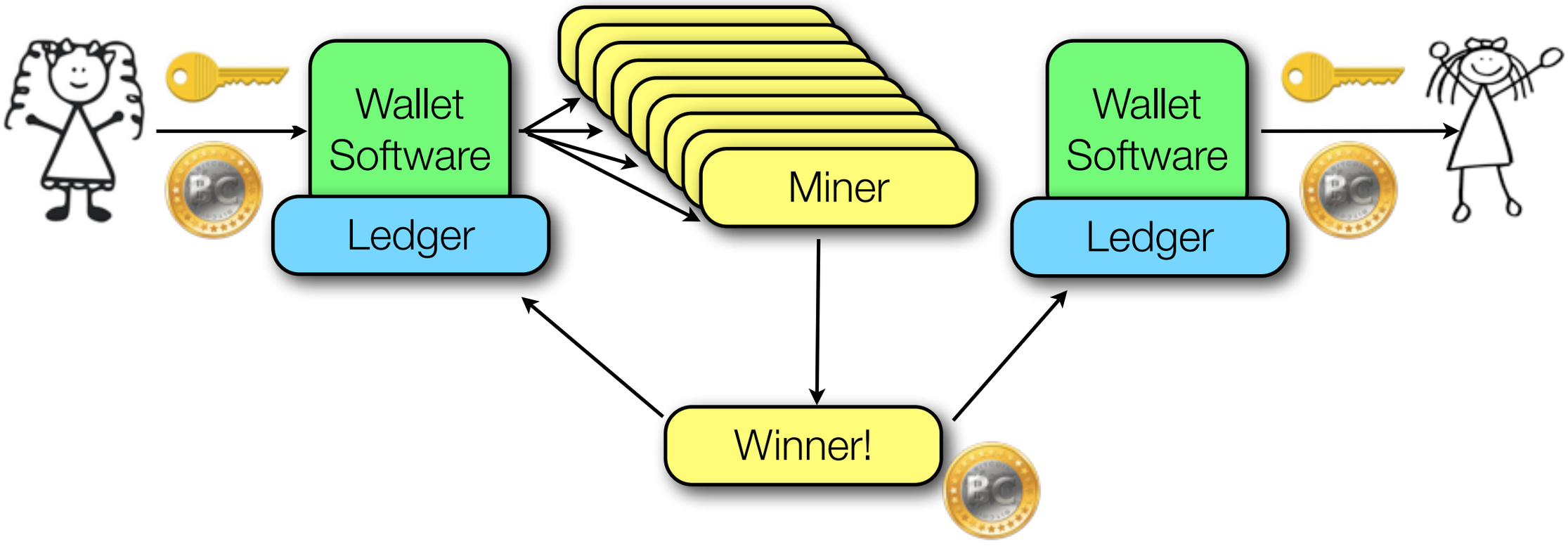
- A special form of ledger, that keeps track of who holds what, that is very, very hard to fraudulently modify
    - What if we have many ledgers, and if some don’t agree, then majority wins.



Idea 2: The Blockchain

- A special form of ledger, that keeps track of who holds what, that is very, very hard to fraudulently modify

    - Miners each update the ledger with recent transactions. One miner with the consensus-agreed correct ledger wins a little math contest they play and get’s to update all the ledgers with their new version.



Crypto-Tech Myths & Facts (Busted)

- There are many understandings and misunderstandings about Crypto-tech.
    - It is NOT anonymous, it’s pseudo-anonymous to a casual observer.
    - Crypto-currency is NOT the preferred currency of criminals. The US $100 bill is.
    - I will lose all my crypto-coin if my exchange goes under, like Mt. Gox.
    - There are hundreds of alternative currencies with different characteristics such as Litecoin, Darkcoin, Dogecoin and Ether.
    - Crypto-currency is not all there is to this technology. Smart Contracts are the really interesting part.

Conclusion

- You can answer most non-technical questions about crypto-technology if you remember:

Public Key Cryptography uses private and public keys and math to make it possible to irrevocably transfer any virtual good between two parties.

The **Blockchain** is a distributed ledger system maintained by consensus that makes it very difficult to fudge the record of who owns what for purposes of theft, for example.

Crypto-technology has many applications, with crypto-currency being just one.

There's much more to learn but basic questions can be answered knowing only the above.

Discussion

Bernd Petak
Consulting

Questions? Thoughts?

Bernd Petak - bernd.petak@gmail.com
Twitter - @berndpetak