Blockchain and its applications

16 November 2016

ISSE 2016 Paris
marc.sel@be.pwc.com
Contents

1. Objectives of this presentation
2. Blockchain applications and business models
3. Blockchain security and trust

Appendix
Objectives of this presentation
Objectives of this presentation

• This presentation discusses the trust model behind blockchain as well as possible business models and applications

• A short functional introduction to blockchain and its underlying principles is provided since this facilitates such understanding greatly
Blockchain applications and business models
Blockchain in a nutshell

• Users interact with applications via a node containing a copy of the blockchain
• Applications perform transactions (e.g. virtual coins, smart contracts)
• Transaction outcomes become stored in every copy of the blockchain
**Blockchain in a nutshell**

- Transactions are stored inside a candidate block 🧑‍💻 🟢 ␣  🔴 🟢 🟢
- Blocks are strongly linked in a chain, starting from the genesis block 
- Every node has a copy of the chain, and extends that copy in an agreed way 
- Once a transaction’s block is part of the chain, it can be considered as immutable, and the transaction as committed 
- Hence the chain acts as a distributed ledger
Blockchain in a nutshell

- Transactions are stored inside a candidate block. This takes place at each node.
- All nodes broadcast their transactions on the network.
- Full nodes have a function referred to as ‘miner’, aiming at solving a cryptographic hash puzzle.
- Puzzle consists of finding a unique number that when inserted in a block, completes the block in such a way that hash(block) conforms to the blockchain’s specification.
- When a ‘miner’ in a particular node is the first to solve the puzzle, his block is broadcasted and verified by all nodes.
- Upon successful verification all nodes extend their copy of the blockchain by the new block.
**Peer2Peer network of nodes, every node has a copy of the blockchain**

A, B, C, D, E are all nodes, connected in Peer2Peer mode.
Smart Contracts

1. Pre-defined contract
   - Terms are established by all counterparties, such as:
     - Variable interest rate (e.g. LIBOR)
     - Currency of payments
     - Currency rate
     - Conditions for execution (e.g. time and date, LIBOR rate at given value)

2. Events
   - Event triggers contract execution
     - Transaction initiated
     - Information received

3. Execute & Value transfer
   - Terms of contract dictate movement of value based on conditions met.

4. Settlement
   - a) On-chain assets (Digital)
     - For digital assets on the chain, such as a cryptocurrency, accounts are atomically settled
   - b) Off-chain assets (Physical)
     - For assets represented off the chain, such as stocks and fiat, changes to accounts on the ledger will match off-chain settlement instructions
Smart Contracts - Example

- Financial Swap

```python
data Alice, Bob
data deadline, threshold

# Not shown: collect equal deposits from Alice and Bob
# We assume StockPriceAuthority is a trusted third party contract that can give us the price of the stock

def determine_outcome():
    if block.timestamp > deadline:
        price = StockPriceAuthority.price()
        if price > threshold:
            send(Alice, self.balance)
        else:
            send(Bob, self.balance)
```

- On-chain if `.balance` is on the chain and payment is in virtual currency
- Off-chain if `.balance` is residing off the chain and the payment is in the contract consists of sending a message to make the real payment
## Blockchain applications – public or private

### Public Blockchain
- No central point of control by individuals, corporations or governments
- Permissionless to participate
- Consensus based on “proof of work”
- Examples:
  - *Bitcoin*
  - *Ethereum*

### Consortium/Hybrid Blockchain
- Controlled by more than two individuals, corporations or governments
- Permission on participation from consortium necessary
- Arbitrary consensus mechanism
- Readability of the blockchain can be public or restricted to the consortium

### Full private Blockchain
- Controlled by one individual, corporation or government
- Permission on participation from owner necessary
- Readability of the blockchain can be public or restricted to one
**Blockchain application “on chain”**

- “On chain” – coins & value bearing contracts
- Value is transferred directly between accounts on the blockchain

Direct execution

Smart contract

\[ T_2 = \text{smart contract that will execute automatically when its conditions are fulfilled} \]
**Blockchain application “off chain”**

- “Off chain” – the digital doppelganger
- Lifecycle events of item in the real world are mirrored on the blockchain
- Value bearing items reside outside (“off”) the blockchain and is uniquely authenticated (gemprint, rfid tag, ...)
- Blockchain contains “rights”
Blockchain application “off chain”

PERMANENT. IMMUTABLE.

Everledger is a permanent ledger for diamond certification & related transaction history. Verification for insurance companies, owners, claimants & law enforcement.
Blockchain security and trust
Security, trust and confidence equation

Blockchain and security

Security of blockchain based applications presents itself as attractive:

1. Integrity:
   • Provided via hash tree
   • Verifiable to all participants

2. Confidentiality: use of pseudonyms (public keys), but what is published on the blockchain is publicly visible – so you may have to:
   • Encrypt selective data elements, or
   • Operate a private blockchain where you can limit access to

3. Availability:
   • Inherently strong via peer-to-peer
   • Provided via replication of the blockchain to all participating nodes
Security, trust and confidence equation

Blockchain and security

In the real world, security is combination of at least cryptographic components, operational processes and legal components. Assurance typically provided from outside (lab, auditor).

*With regard to operational and legal components, blockchain based applications are not yet at the same level of maturity of ‘traditional’ applications. Also the provision of assurance is still a research topic more than anything else.*
Security, trust and confidence equation

Blockchain and trust

Consensus of the participants: ‘majority decides’, but since we deal with pseudonyms it is not guaranteed what the majority is composed of (limited control)

The code: open source code that can be scrutinised, content of the blockchain is publicly visible as well. It has been demonstrated that code despite exposure and multiple reviews may still contain weaknesses:

- The weaknesses that remained in TrueCrypt despite multiple review rounds, triggered the creation of VeraCrypt
- The DAO hack of June 2016 (limited control)

The people managing the code: are humans, subject to legislation. Legislation in a global context can be qualified as complex (limited control)
Further information

maxim.deboiserie@be.pwc.com

sander.demeester@be.pwc.com

marc.sel@be.pwc.com – www.marcsel.eu
Appendix
Further references

http://mapofcoins.com
http://www.blockexplorer.com
http://www.ethernodes.org
https://www.w3.org/community/blockchain/
http://r3cev.com/ – R3 – financial services based on blockchain
http://ripple.com/ – Ripple – financial services based on blockchain
https://www.ethereum.org/
https://daohub.org/
http://szabo.best.vwh.net/smart_contracts_idea.html
https://wiki.mozilla.org/Badges/
https://ethident.com

Stephan Tual - Blockchain beyond Bitcoin - Lift 2016:
https://www.youtube.com/watch?v=CnUdwxZsyXc

Top 10 Start-ups:
https://medium.com/the-intrepid-review/the-top-10-blockchain-startups-to-watch-in-2016-the-leaders-who-are-changing-the-game-6195606b0d70#hiyg15hs1