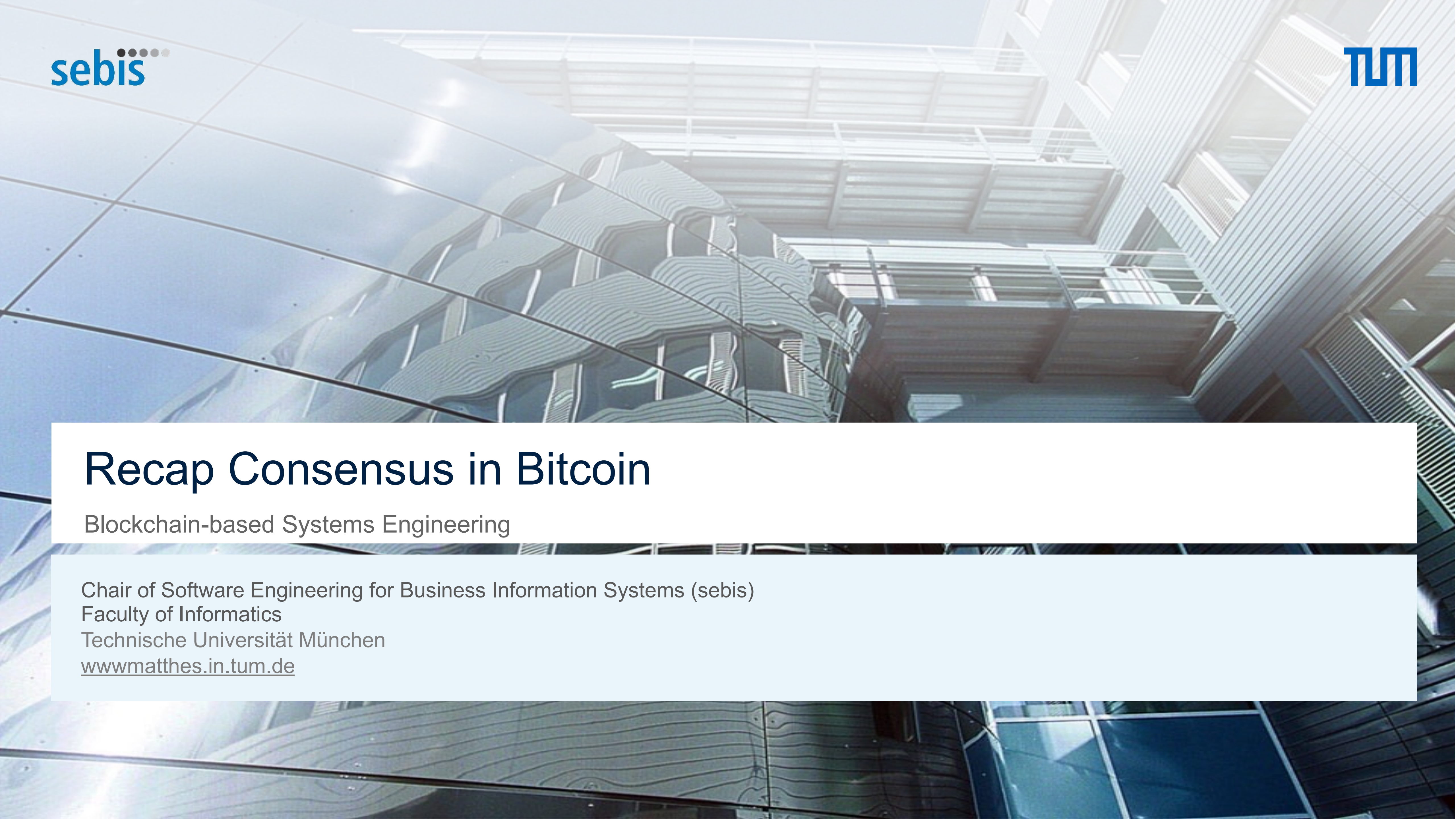


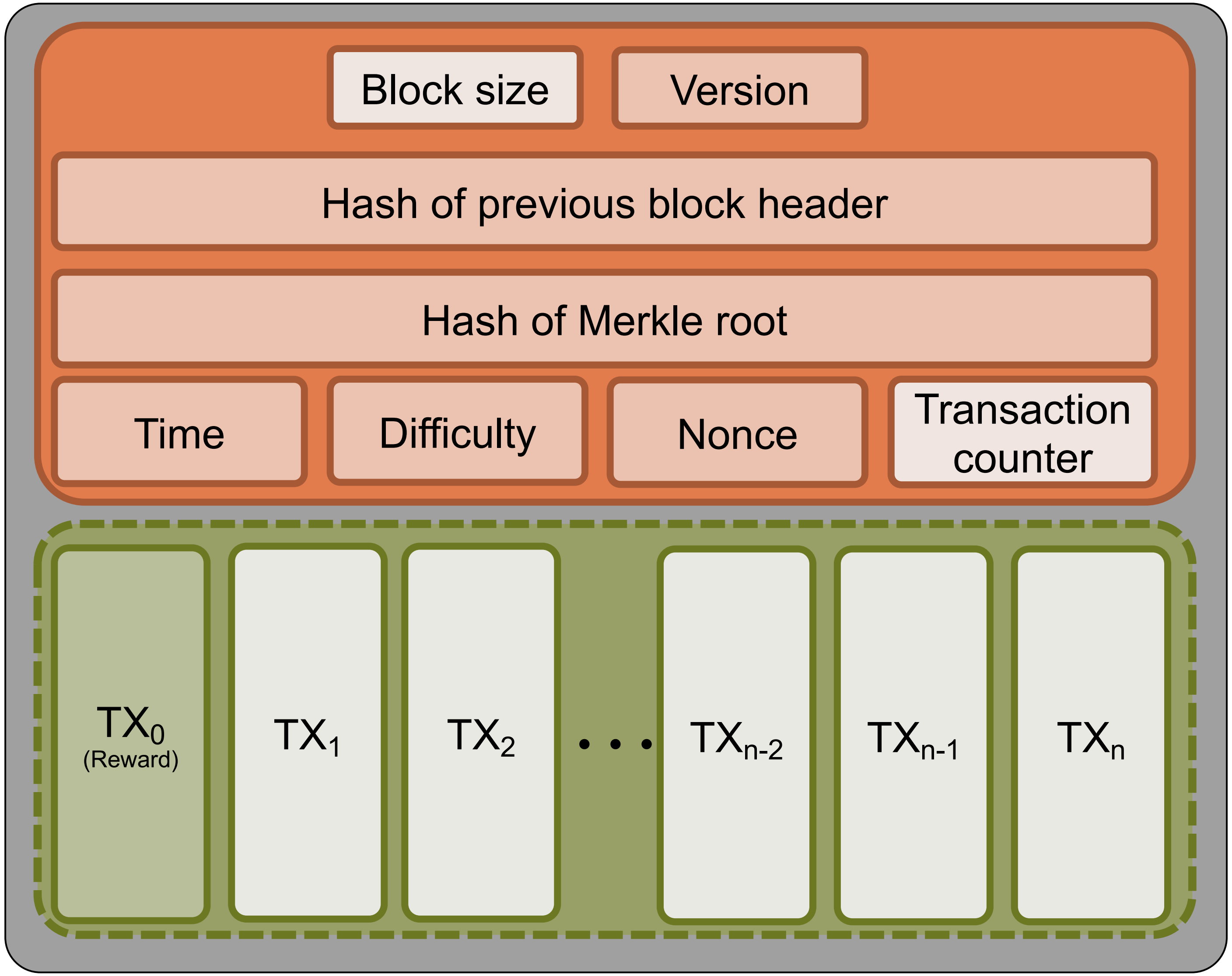
Recap Consensus in Bitcoin

Blockchain-based Systems Engineering

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
wwwmatthes.in.tum.de

Block Details

- The *hash of the previous* block creates the chaining.
- The hash of the Merkle root node of a Merkle tree structure with all transactions (as explained in Chapter 2).
- The *nonce* is required for the consensus mechanism in the network.
- The block‘s hash used for chaining is calculated from the *version* until the *nonce* field.
- The height of the block is stored in the coinbase transaction. (TX_0)



Difficulty Calculation & Block Time

- The block time defines the average time between the creation of two blocks (In Bitcoin, block time = 10 minutes)
- Why has the block time to be constant?
  - Too slow:
    - Transactions take longer to be included
    - Network capacity decreases
  - Too fast:
    - Higher possibility of chain forking, leading to multiple “realities”.
    - Network has to keep track of these forks even if many will be orphaned.
    - Empty blocks
- How do we design the search puzzle in such way that it keeps a constant block time?
- Every 2016 blocks, the difficulty of the puzzle is adapted to the current network speed.
- The longest chain is considered as the chain with the accumulated highest difficulty.

1 Measure, how long the last 2016 blocks took to get mined. (=T)

2 Calculate the factor of speed (two Weeks / T) (=F)

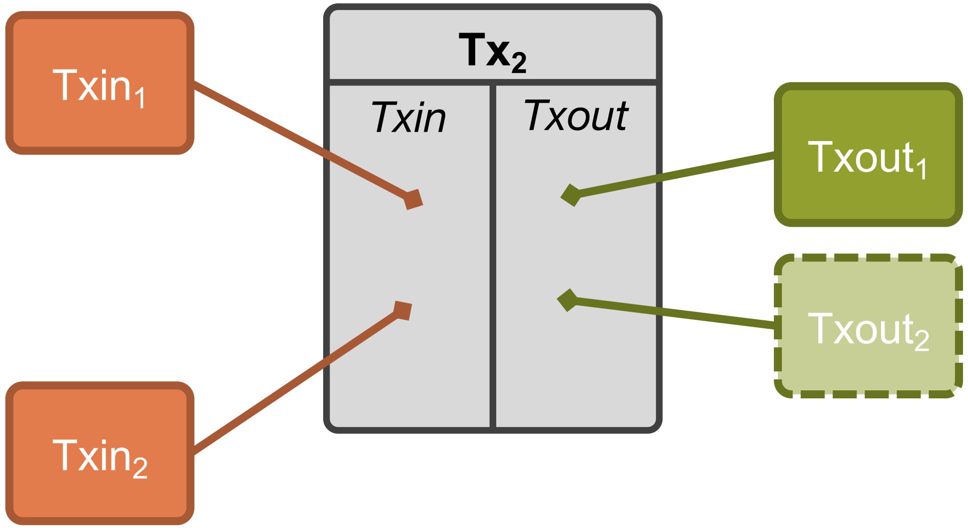
3 The difficulty gets increased (F > 1) or decreased (F < 1).

3a Maximum increase: 4. Maximum decrease: 0,25.

4 The process is done every 2016[1] blocks.

[1] 14 Days x 24 Hours x 6 (every 10 mins) = 2016

Transaction-based Ledger

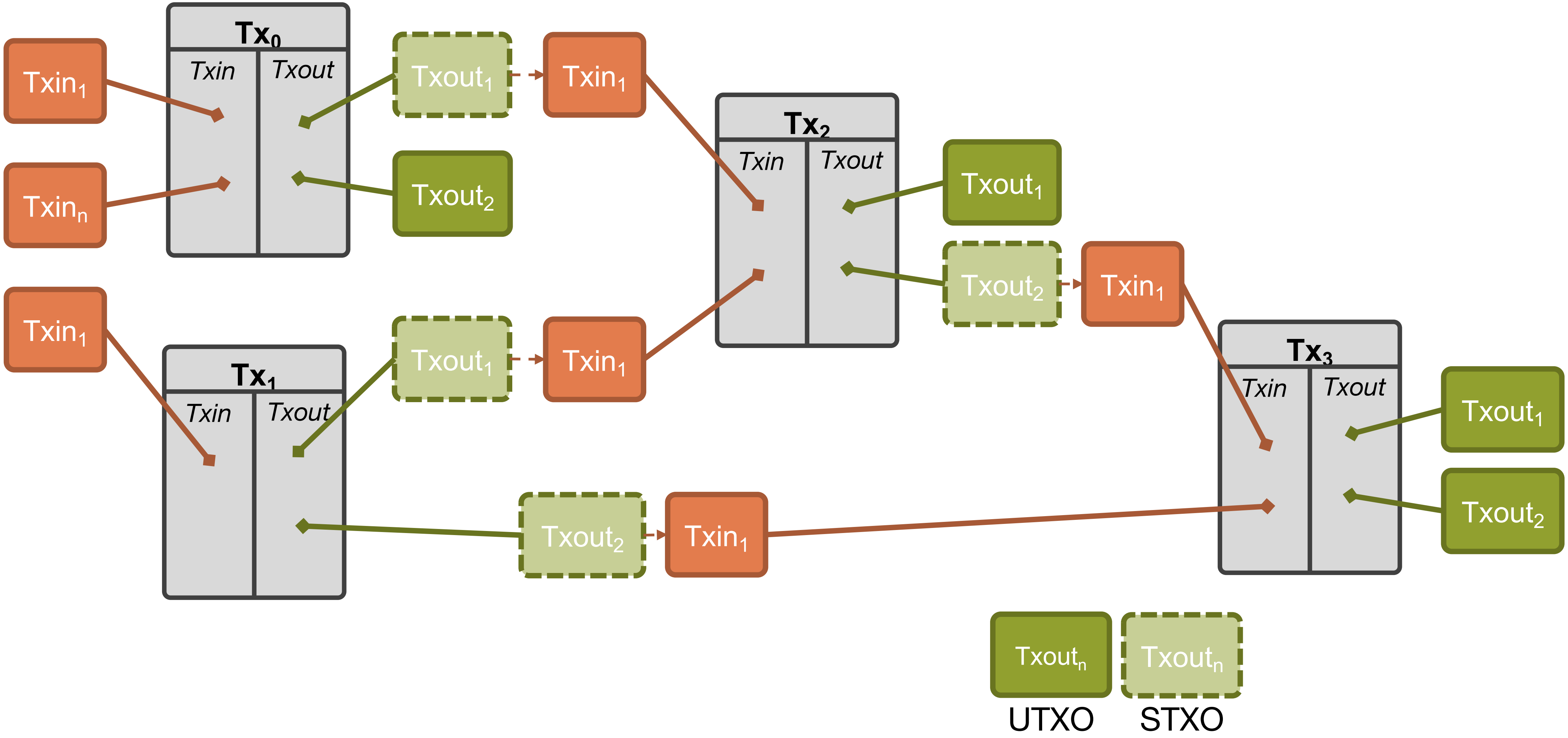


- Transactions (**Tx**) have a number of inputs and a number of outputs.
  - **Inputs (Txin)**: Former outputs, that are being consumed
  - **Outputs (Txout)**: Creation of new coins and transfer of coin ownership

- In transactions where **new coins** are created, **no Txin** is used (no coins are consumed)

- Each transaction has a unique identifier (**TxID**). Each output has a unique identifier within a transaction. We refer to them (in this example) as *#TX[#txout]*, e.g., 1[1], which is the second Txout of the second transaction.

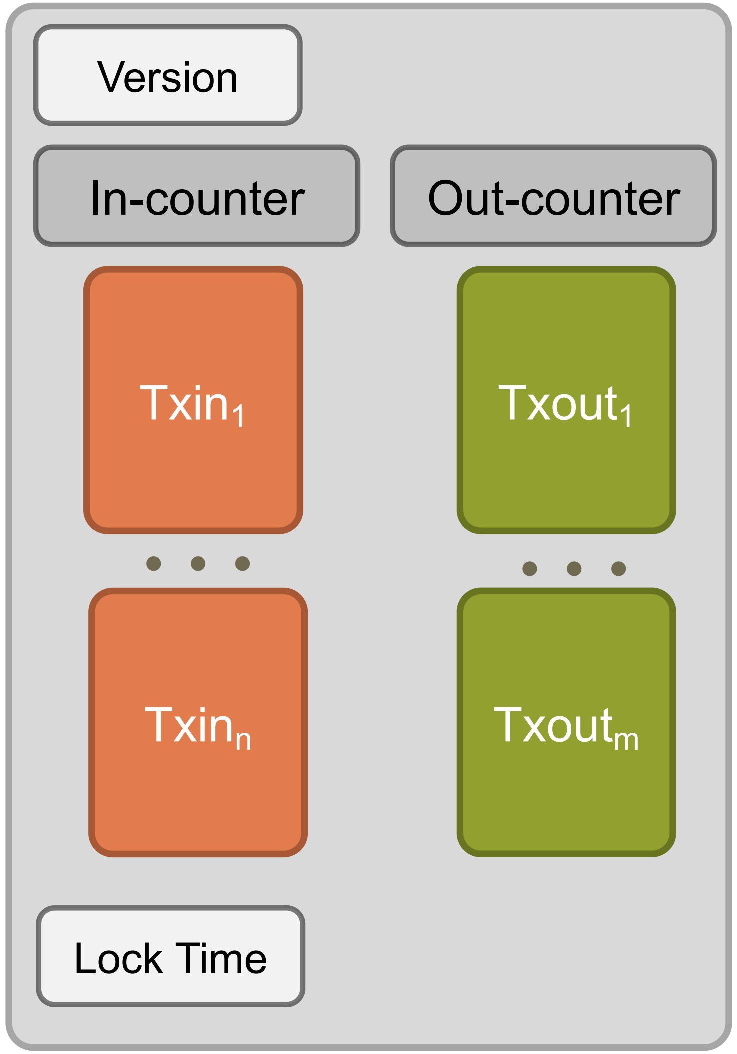
Transactions Connected by Inputs and Outputs



An Advanced Look at Transactions

As previously stated, transactions consist of inputs and outputs following these principles:

- All inputs reference an existing unspent output or a coinbase transaction.
- Inputs and outputs **contain scripts** (scriptSig, scriptPubKey) **for verification**.
- Output scripts (scriptPubKey) **specify the conditions to redeem their value**.
- Input scripts (scriptSig) **provide a signature** to redeem the referenced output.
- Only **outputs store** the **BTC value** and the **receiver‘s address**.
- **All coins have a history (inputs/outputs) up to the original coinbase transaction that created them.**



Input format

Txin

- previous transaction hash
- previous Txout-index
- script length
- *scriptSig*

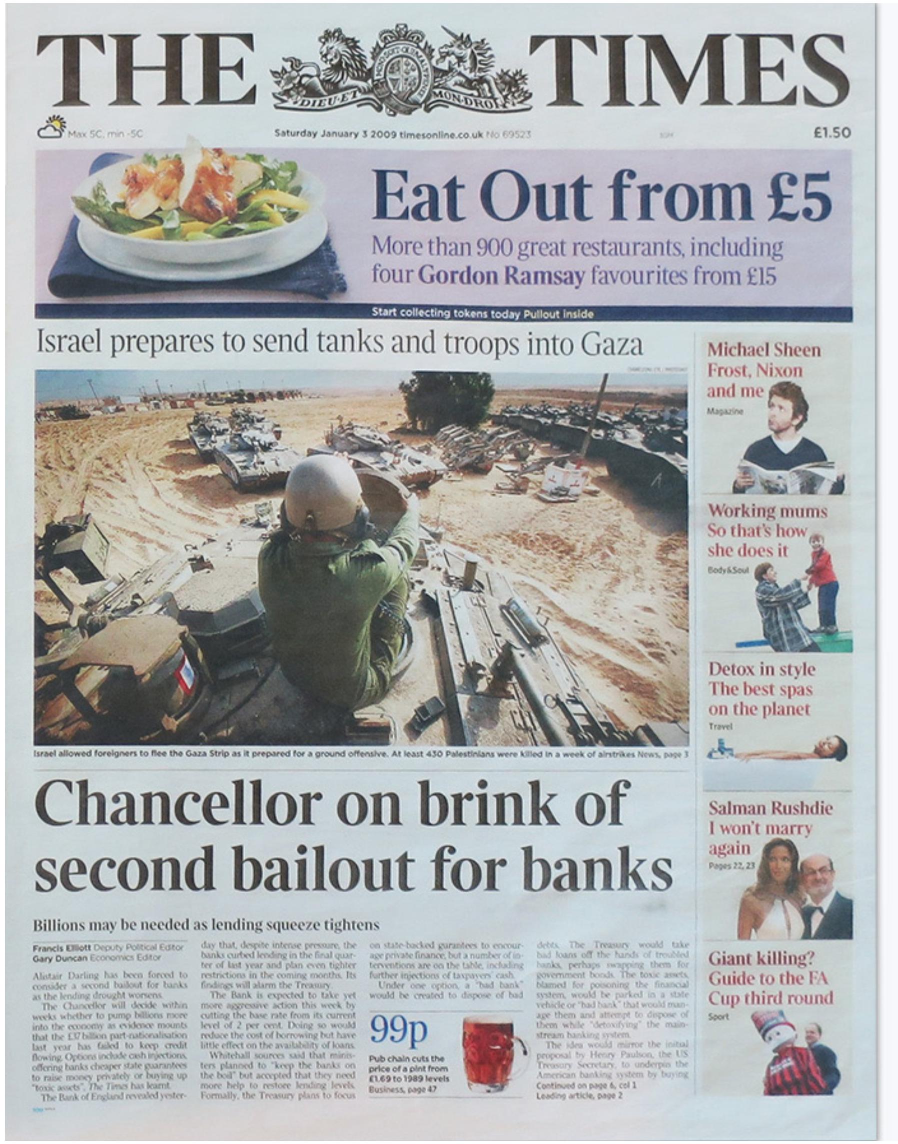
Output format

Txout

- value in *Satoshi (=10^{-8} BTC)*
- script length
- *scriptPubKey*

© sebis

Data Contained in the Genesis Block



THE TIMES

DIEU ET MON DROIT

Max 5C, min -5C

Saturday January 3 2009 timesonline.co.uk No 69523

£1.50

Eat Out from £5

More than 900 great restaurants, including four **Gordon Ramsay** favourites from £15

Start collecting tokens today Pullout inside

Israel prepares to send tanks and troops into Gaza

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes News, page 3

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", *The Times* has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed guarantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1989 levels
Business, page 47

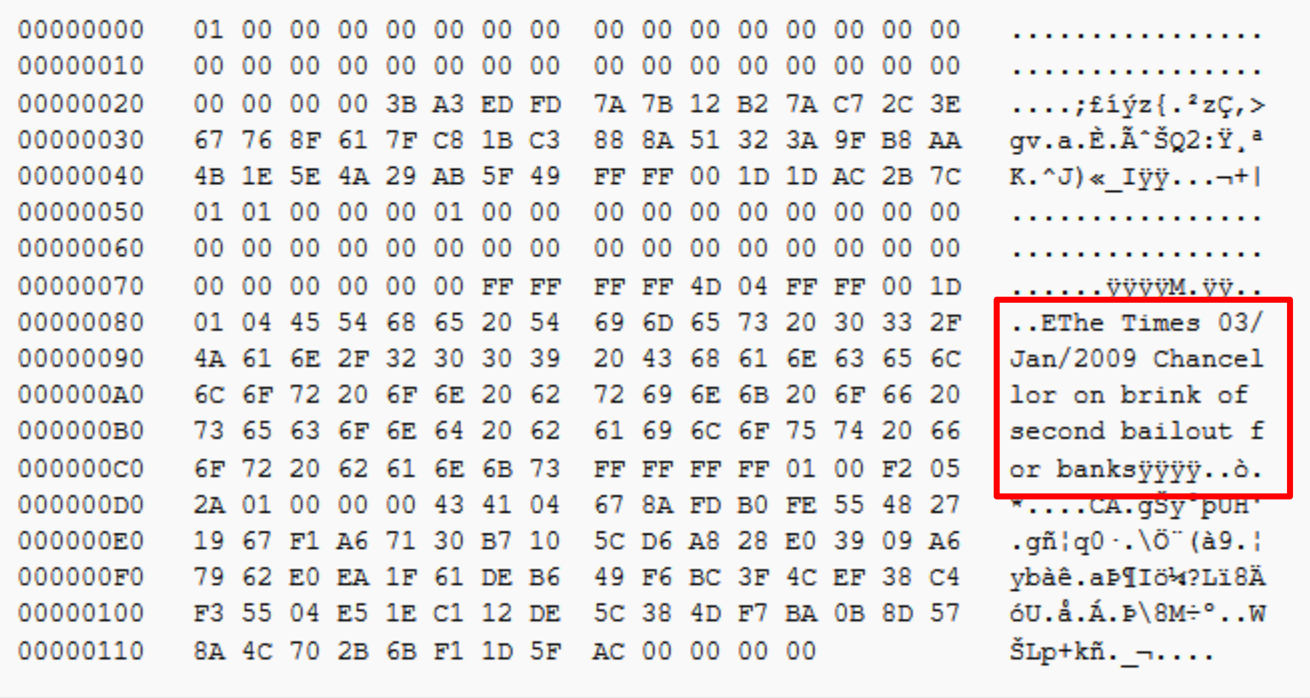
Michael Sheen
Frost, Nixon and me
Magazine

Working mums
So that's how she does it
Body&Soul

Detox in style
The best spas on the planet
Travel

Salman Rushdie
I won't marry again
Pages 22, 23

Giant killing?
Guide to the FA Cup third round
Sport



```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of 
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```

The data highlighted is stored in the *scriptSig* field of the first transaction (=coinbase transaction).

A possible motivation to put this headline into the genesis block is to prove that no "pre-mining" has happened.

Bitcoin Invented a New Approach

- Bitcoin's approach to decentralized consensus was completely new and very different from older approaches that resembled traditional voting and scaled very poorly to more than a handful of nodes.

Ongoing consensus

Sybil Control Mechanism

Incentives

Probabilistic consensus:
The consensus mechanism is an ongoing process in Bitcoin. Therefore, the order of blocks or transactions is never 100% final.

Proof-of-Work:
The network selects a random node to propose a new block using Proof-of-Work. As we will see later, this ensures that probabilistic consensus can be reached assuming over 50% are honest.

Incentivized nodes:
The network incentivizes nodes to participate in the consensus algorithm. They receive Bitcoins for created blocks which are included in the longest chain.