



BLOCKCHAIN 2

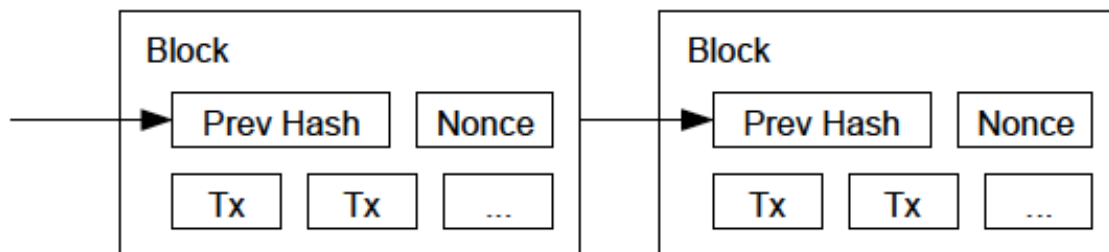
Murat Osmanoglu

BITCOIN

4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority

BITCOIN

- A hash function is any function that can be used to map digital data of arbitrary size to digital data of fixed size(MD5, SHA1, SHA256)
- slight differences in input data producing very big differences in output data.
- For example, the MD5 hashes of 'abc' compared to 'abC'

abc

0bee89b07a248e27c83fc3d5951213c1

abC

2217c53a2f88ebadd9b3c1a79cde2638

BITCOIN



Puzzle



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.



m_1
 m_2
.

1,2,...
x

HASH

00000000002ed39hs4890123jk...

10 sıfır



Puzzle



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.



Puzzle



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.

Proof of Work

BITCOIN



Puzzle



Ali	20.2
Bülent	13
Necla	3.12
·	·
·	·
·	·



m_1
 m_2
·
·

1,2,...
x

HASH

00000000002ed39hs4890123jk...

10 sıfır



Puzzle

Proof of Work



Ali	20.2
Bülent	13
Necla	3.12
·	·
·	·
·	·



Puzzle




Ali	20.2
Bülent	13
Necla	3.12
·	·
·	·
·	·

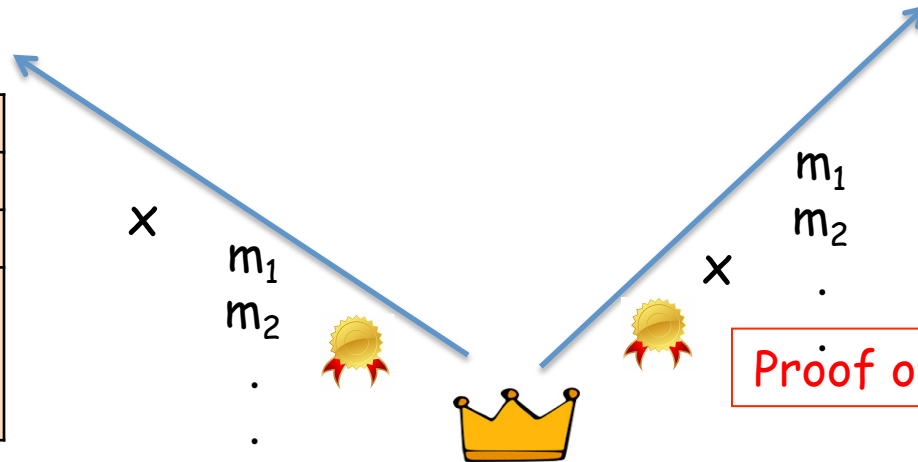
BITCOIN



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.

BITCOIN

$$H(m_1, \dots || x) < T$$

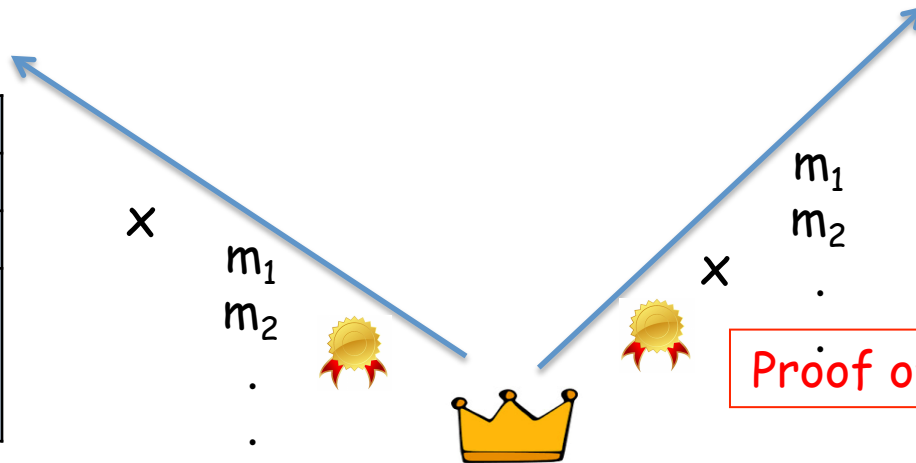


$$H(m_1, \dots || x) < T$$



Ali	20.2
Bülent	13
Necla	3.12
·	·
·	·
·	·

Ali	20.2
Bülent	13
Necla	3.12
·	·
·	·
·	·

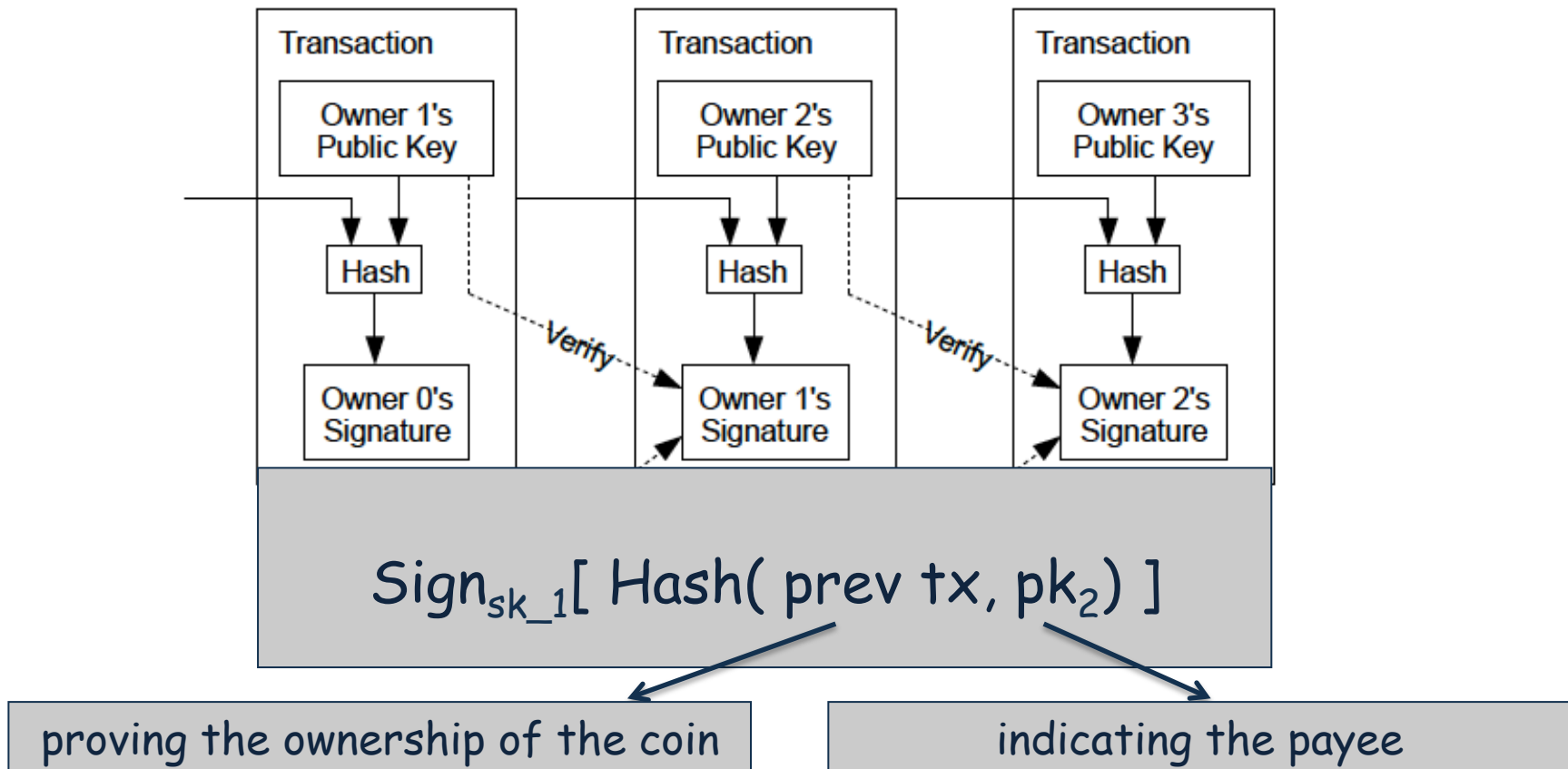


Ali	20.2
Bülent	13
Necla	3.12
·	·
·	·
·	·

BITCOIN

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.



BITCOIN

confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

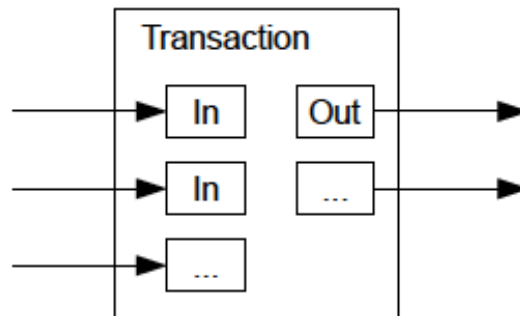
9. Combining and Splitting Value

Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.

- A bitcoin can be divided down to 8 decimal places.
- 0.00000001 BTC (Satoshi) is the smallest amount that can be handled in a transaction

BITCOIN

Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



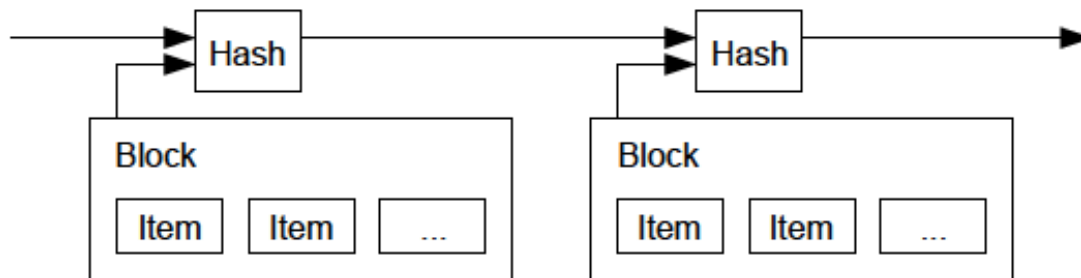
It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

BITCOIN

order in which they were received. The payer needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



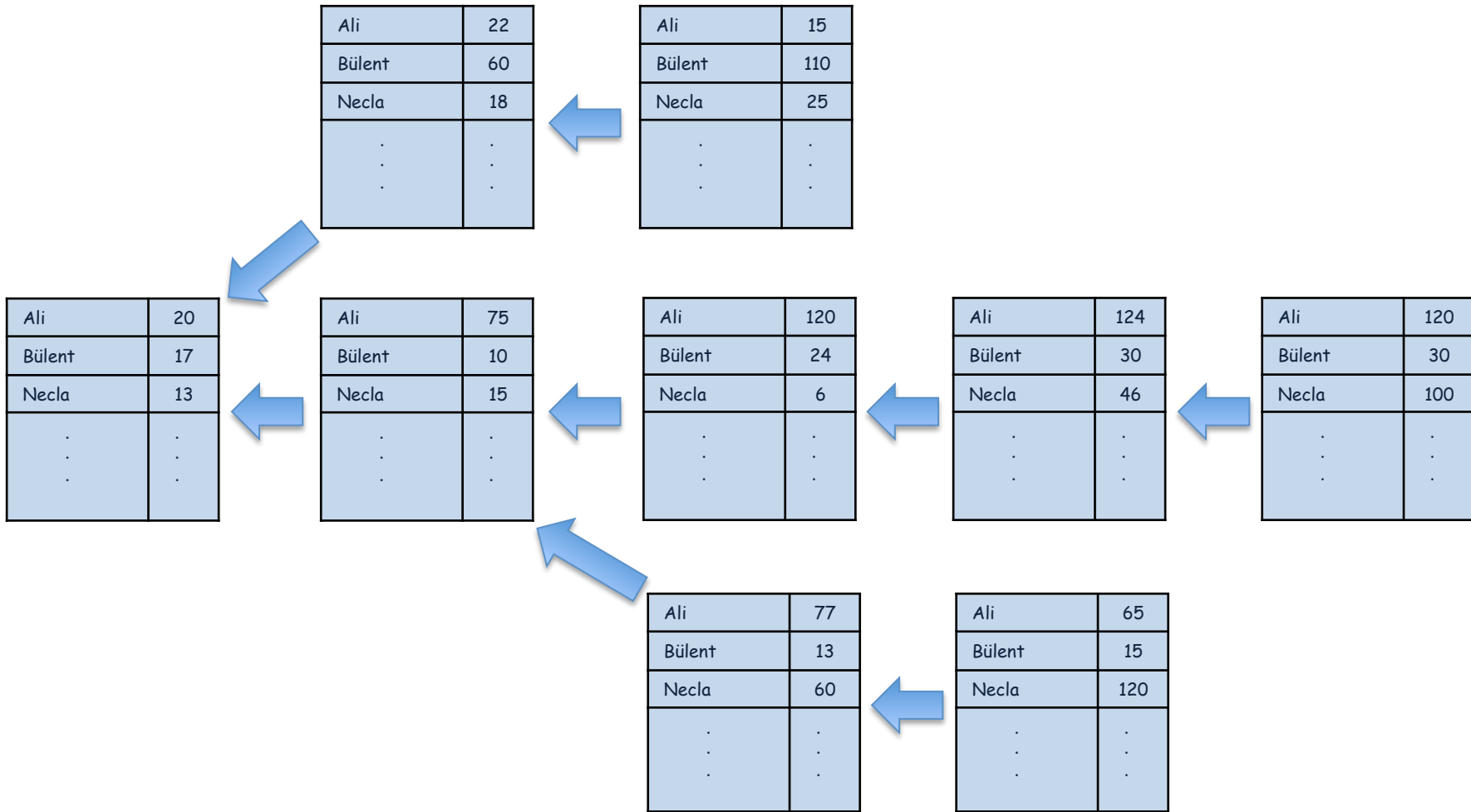
- SHA-256 is used as hash function, which is collision-resistant
- It's hard to find x and y such that $H(x) = H(y)$

BITCOIN

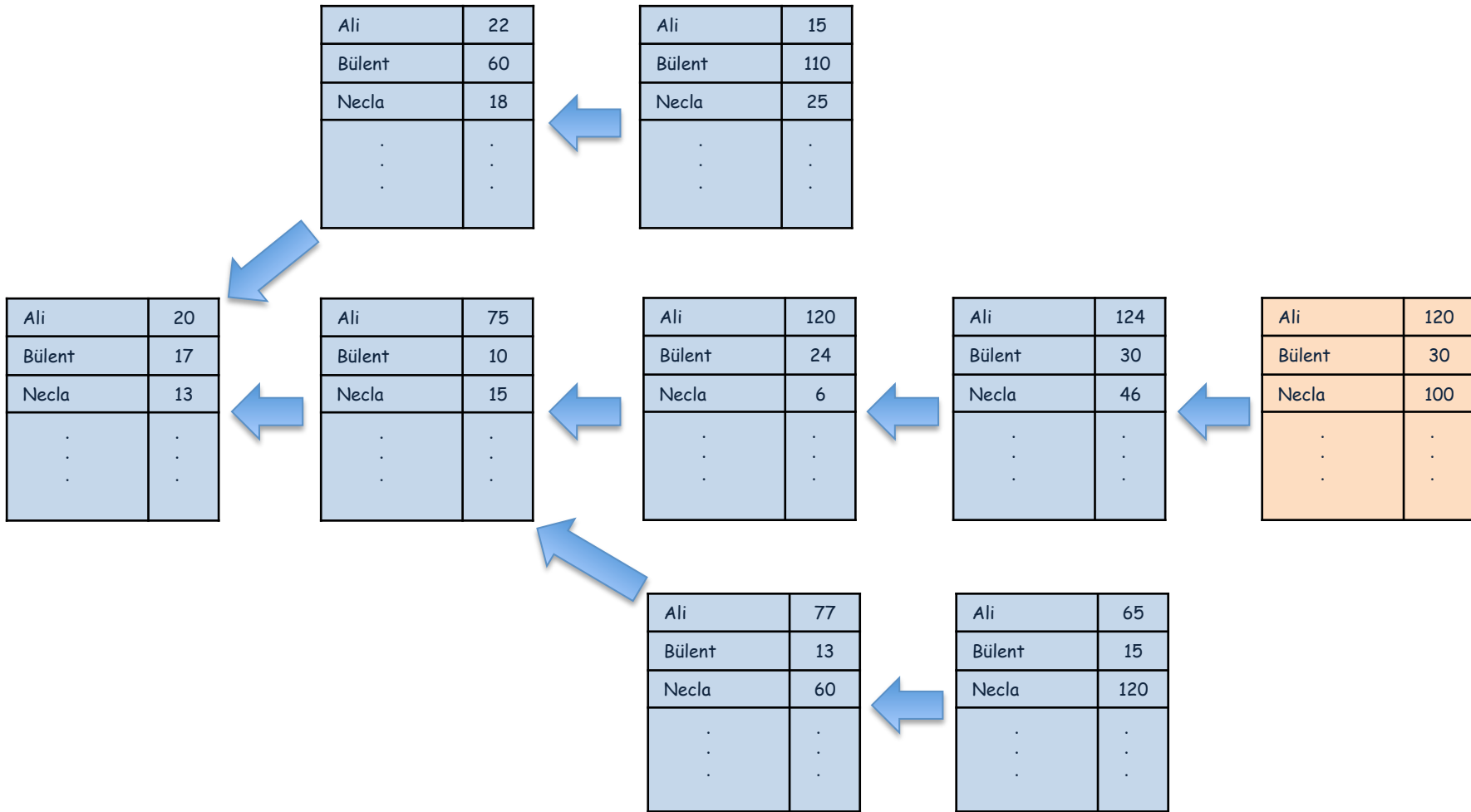
- 3) Each node works on finding a difficult proof-of-work for its block.
- 4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
- 5) Nodes accept the block only if all transactions in it are valid and not already spent.
- 6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

BITCOIN



BITCOIN



BITCOIN

Double-spending

...ing. As the majority, they cannot be outvoted, and are able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

- 1) New transactions are broadcast to all nodes.
- 2) Each node collects new transactions into a block.

BITCOIN

Double-spending

Ali	200
Bülent	170
Necla	880
.	.
.	.
.	.

Ali sends 800 bitcoins to Necla 🏆

Ali	1000
Bülent	170
Necla	130
.	.
.	.
.	.

Ali	0
Bülent	1170
Necla	180
.	.
.	.
.	.

Ali	0
Bülent	1170
Necla	180
.	.
.	.
.	.

Ali	0
Bülent	1170
Necla	180
.	.
.	.
.	.

Ali	0
Bülent	1170
Necla	180
.	.
.	.
.	.

It suggests to wait 6 blocks to confirm a tx

Ali sends 1000 bitcoins to Bulent 🏆

BITCOIN

in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

- 1) New transactions are broadcast to all nodes.
- 2) Each node collects new transactions into a block.
- 3) Each node works on finding a difficult proof-of-work for its block.
- 4) When a node finds a proof-of-work, it broadcasts the block to all nodes.

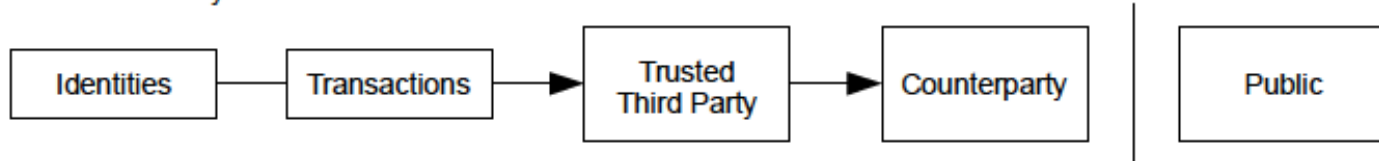
$$H(tx_1 \dots tx_n \parallel x) < T$$

BITCOIN

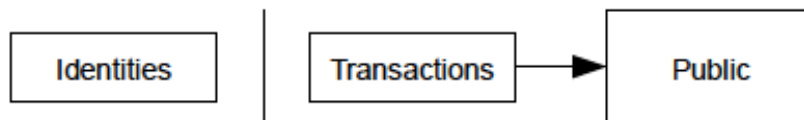
10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.

Traditional Privacy Model



New Privacy Model



BITCOIN



$h(PK)=1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX.$

SK PK

1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX	32
18RcfsA8S2G3AQcJqBEnaDFc2Mb16SKRsE	12
12gtdfsgNvrDWxgDrJi38M5M2oAUGJcNMS	45
·	·
·	·
·	·

- identities are hidden

BITCOIN

- The reward is cut in half every four years (210.000 blocks)
- At the beginning (2009), the reward was 50 BTC. (Now 6.25 BTC)
- Around 2140, it drops below 1 satoshi, and no more creation after that (1 BTC = 100.000.000 satoshi)
- It promises scarce token economy with an eventual cap of about 21M bitcoins

BITCOIN

- A protocol that supports a decentralized, pseudo-anonymous, peer-to-peer digital currency
- A publicly disclosed linked ledger of transactions stored in a blockchain
- A reward driven system for achieving consensus (mining) based on "Proofs of Work" for helping to secure the network

BITCOIN

History

2008

- August 18 Domain name "bitcoin.org" registered
- October 31 Bitcoin design paper published
- November 09 Bitcoin project registered at SourceForge.net

2009

- January 3 Genesis block established at 18:15:05 GMT
- January 9 Bitcoin v0.1 released and announced on the cryptography mailing list
- January 12 First Bitcoin transaction, in block 170 from Satoshi to Hal Finney

What is Blockchain?

- a decentralized, distributed database(ledger) that is used to maintain a continuously growing list of records (transactions).
- enables transactions to be pooled into blocks and recorded
- allows the resulting database(ledger) to be accessed by the different parties
- cryptographically chains blocks in chronological order

What is Blockchain?

- In blockchain, all parties agree on a specific protocol that determines true state of the database(ledger) at any point in time.
- initiation and broadcasting the transaction
(digital signatures with secret-public key pairs)
- validation and recording of the transactions
(digital signatures and consensus mechanism)
- chaining blocks
(hash function)

What is Blockchain?

- It can be used without a central authority by individuals or entities with no basis to trust each other
- It can be used to create value or issue assets
- It can be used to transfer value or the ownership of assets
- It can be used to record those transfers of value or ownership of assets