Distributed Ledger Technology Workshop

1° febbraio 2018 Università degli Studi di Perugia

Blocks and **Fees** in **Bitcoin**

[Observationally Speaking]

Marco **Benedetti**, Gennaro **Catapano**, Francesco **De Sclavis***, Roberto **Favaroni**, Giuseppe **Galano**, Andrea **Gentili**, Marco **Mori**

[NAME].[SURNAME]@bancaditalia.it

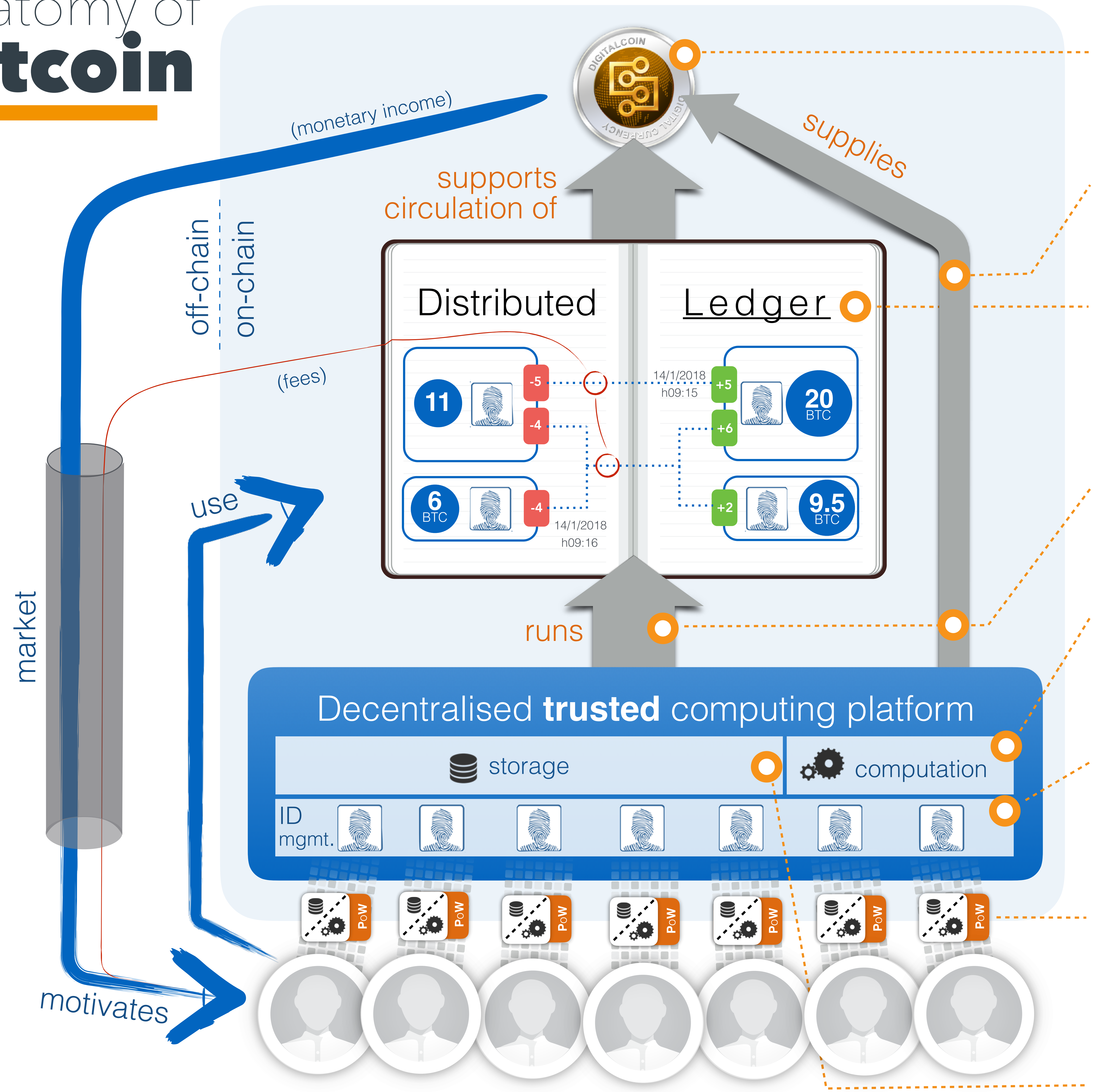
ART
www.bankit.art

*Intern at ART

BANCA D'ITALIA
EUROSISTEMA

The **opinions** expressed and conclusions drawn are those of the **authors** and do **not** necessarily reflect the views of the **Bank of Italy**.

Anatomy of **Bitcoin**



Virtual currency
- aka, cryptocurrency
- aka, mathematical currency
- internal unit of account

Mining
- Predefined supply curve
- Decreasing rate of growth
- "Seigniorage" to participants

No double-spending
- Prevent the same token from being used twice or more

Distributed application
- e.g., Bitcoin
- several other (monetary & non-monetary) proposals

Consensus protocol
"*In case of multiple/inconsistent blockchains, every node must prefer the one backed by the most work*"

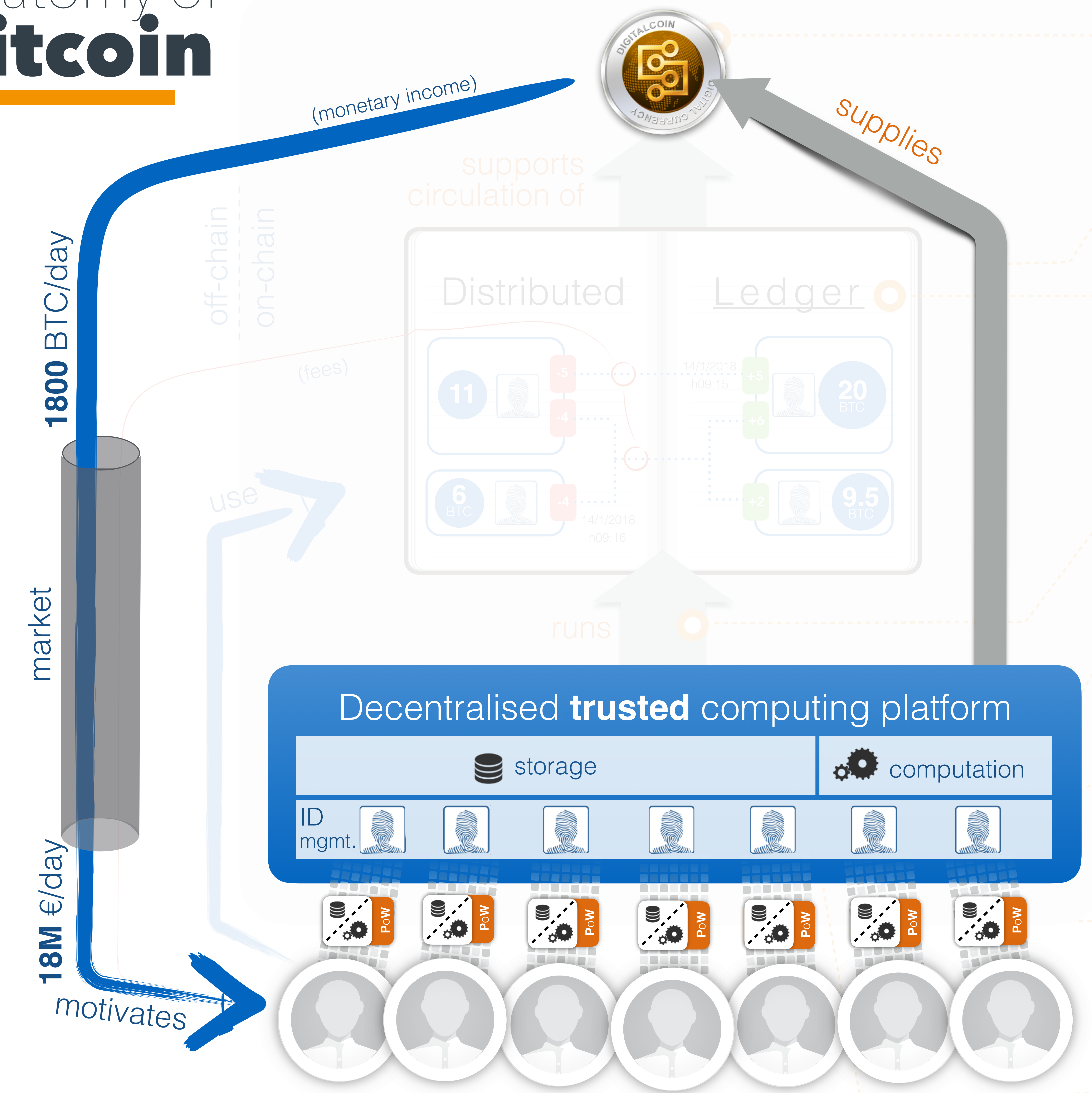
User addresses/identities
- self-generated
- no central registry; no clearance

Based on:
➡Public-Key Cryptography

Proof of work
"*Contributions accepted only if corroborated by evidence of hard, express, dedicated work (fee)*"
Based on:
➡Cryptographic Hash Functions

Blockchain

Anatomy of **Bitcoin**



Virtual currency
- aka, cryptocurrency
- aka, mathematical currency
- internal unit of account

Mining
- Predefined supply curve
- Decreasing rate of growth
- "Seigniorage" to participants

No double-spending
- Prevent the same token from being used twice or more

Distributed application
- e.g., Bitcoin
- several other (monetary & non-monetary) proposals

Consensus protocol
"*In case of multiple/inconsistent blockchains, every node must prefer the one backed by the most work*"

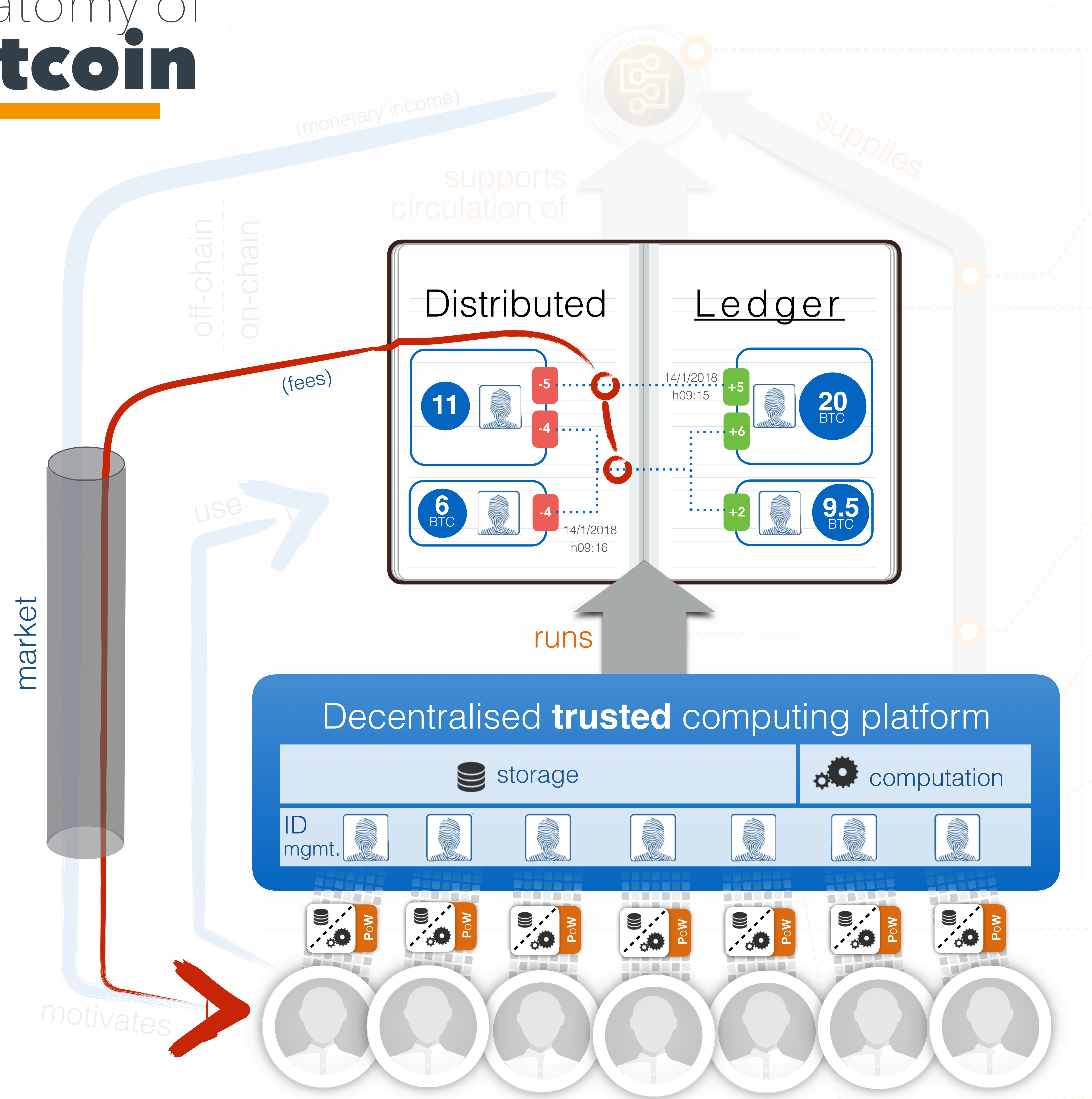
User addresses/identities
- self-generated
- no central registry; no clearance

Based on:
➡Public-Key Cryptography

Proof of work
"*Contributions accepted only if corroborated by evidence of hard, express, dedicated work (fee)*"
Based on:
➡Cryptographic Hash Functions

Blockchain

Anatomy of **Bitcoin**



Virtual currency
- aka, cryptocurrency
- aka, mathematical currency
- internal unit of account

Mining
- Predefined supply curve
- Decreasing rate of growth
- "Seigniorage" to participants

No double-spending
- Prevent the same token from being used twice or more

Distributed application
- e.g., Bitcoin
- several other (monetary & non-monetary) proposals

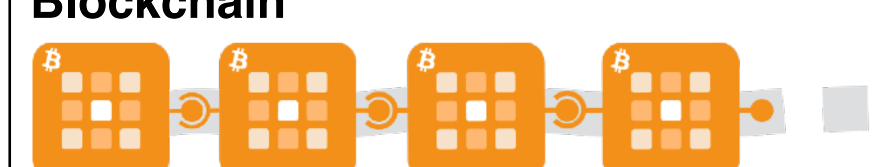
Consensus protocol
"*In case of multiple/inconsistent blockchains, every node must prefer the one backed by the most work*"

User addresses/identities
- self-generated
- no central registry; no clearance

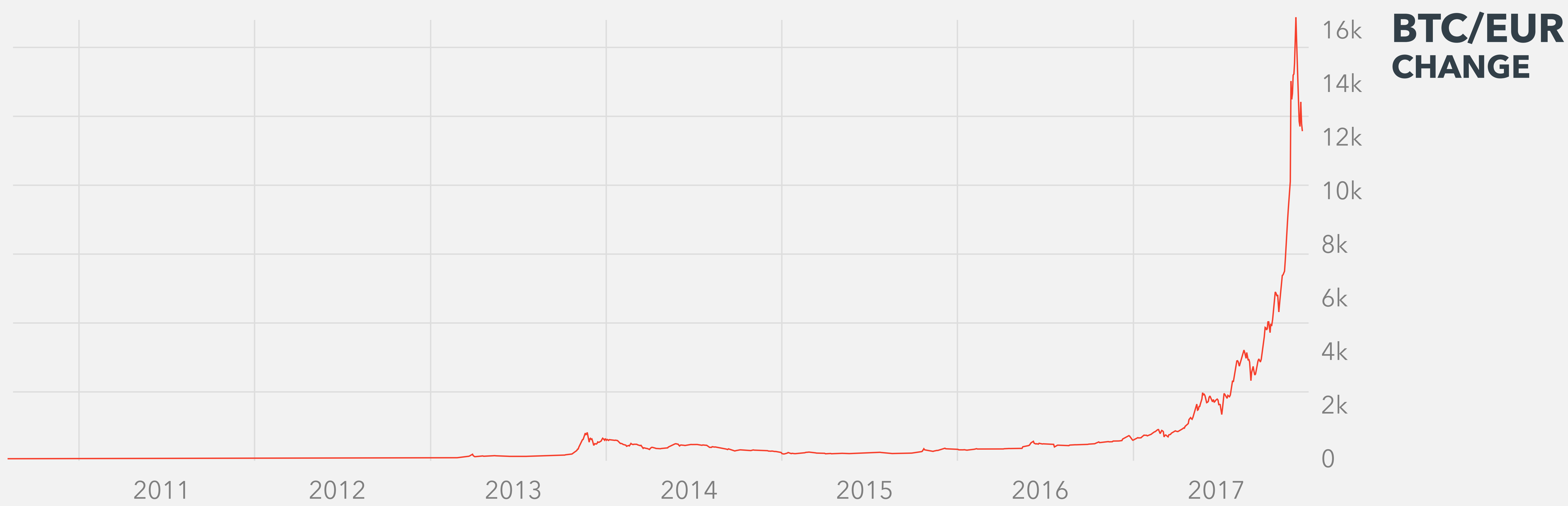
Based on:
➥Public-Key Cryptography

Proof of work
"*Contributions accepted only if corroborated by evidence of hard, express, dedicated work (fee)*"
Based on:
➥Cryptographic Hash Functions

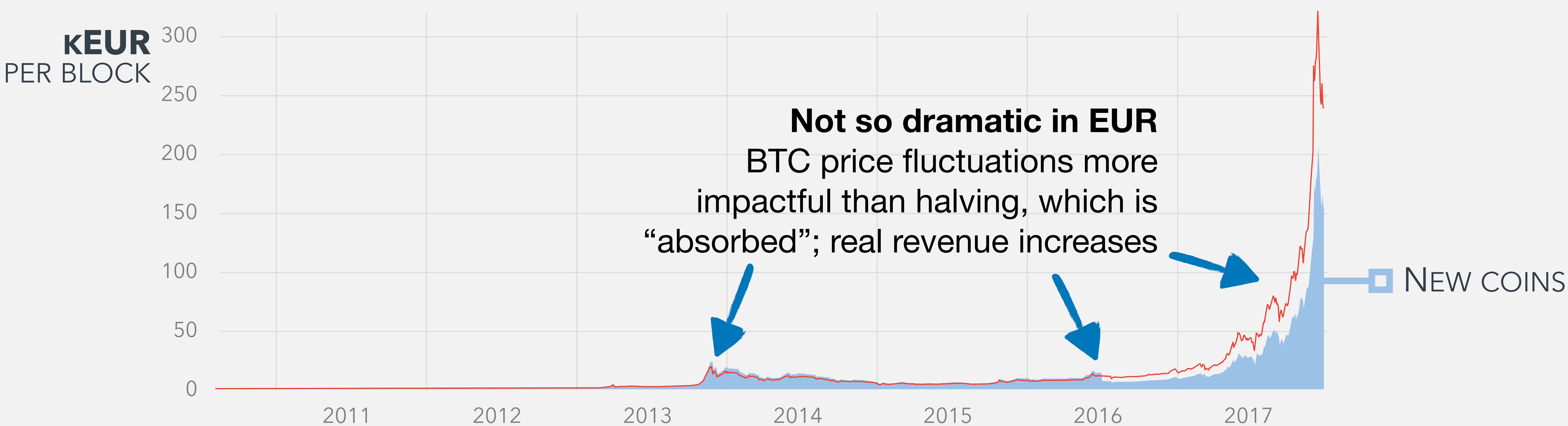
Blockchain



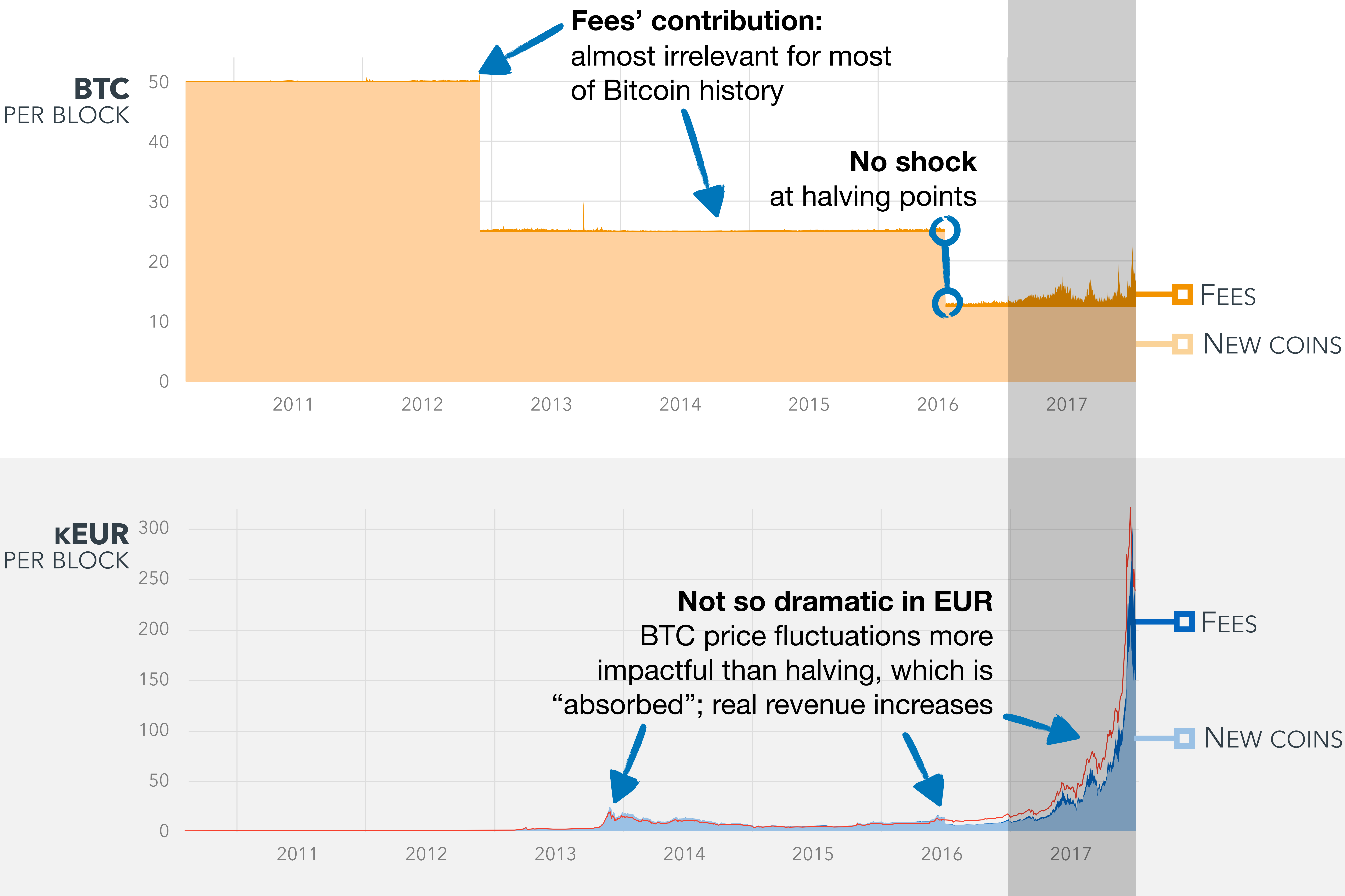
Mining revenues (2011-17)



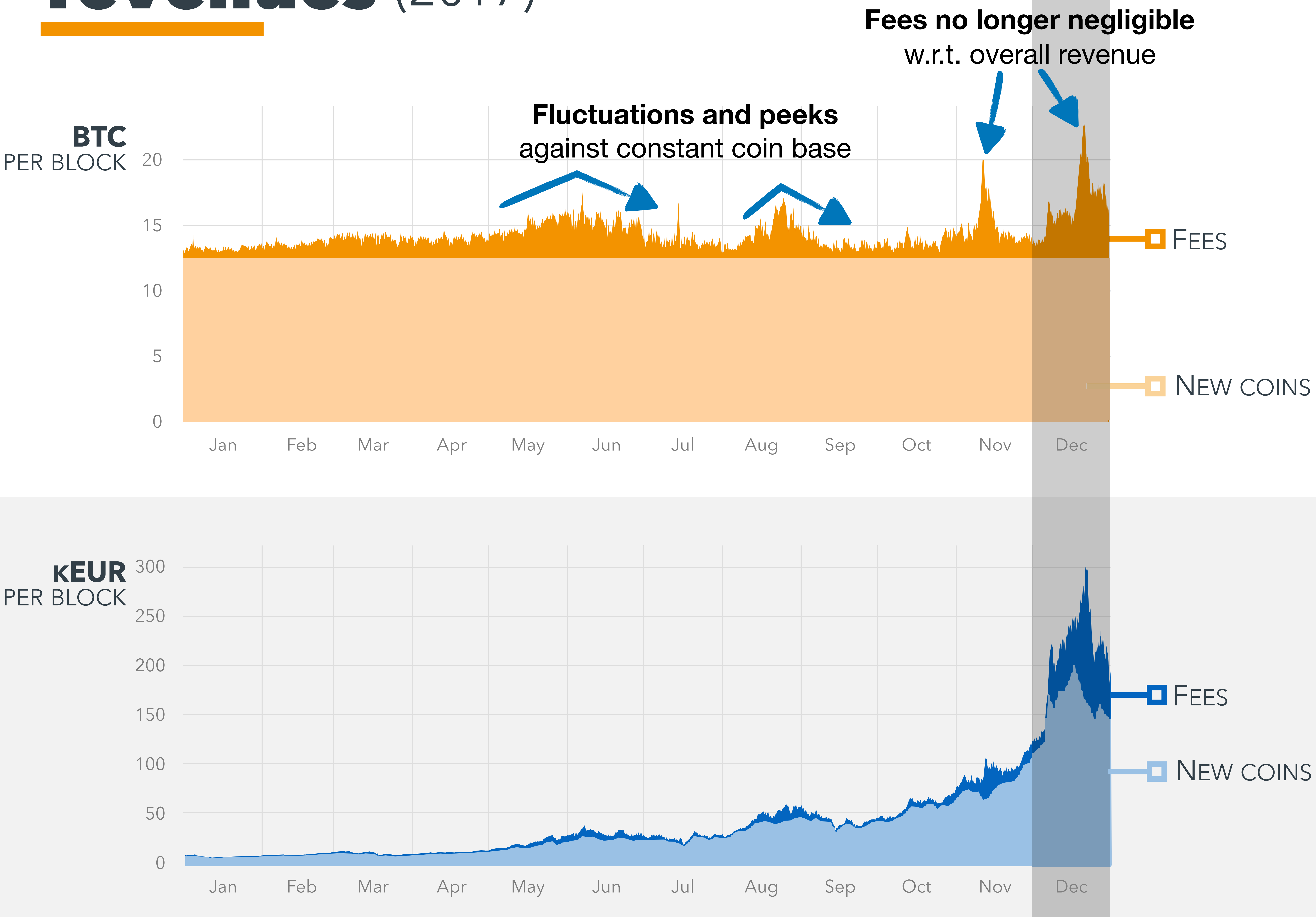
Mining revenues (2011-17)



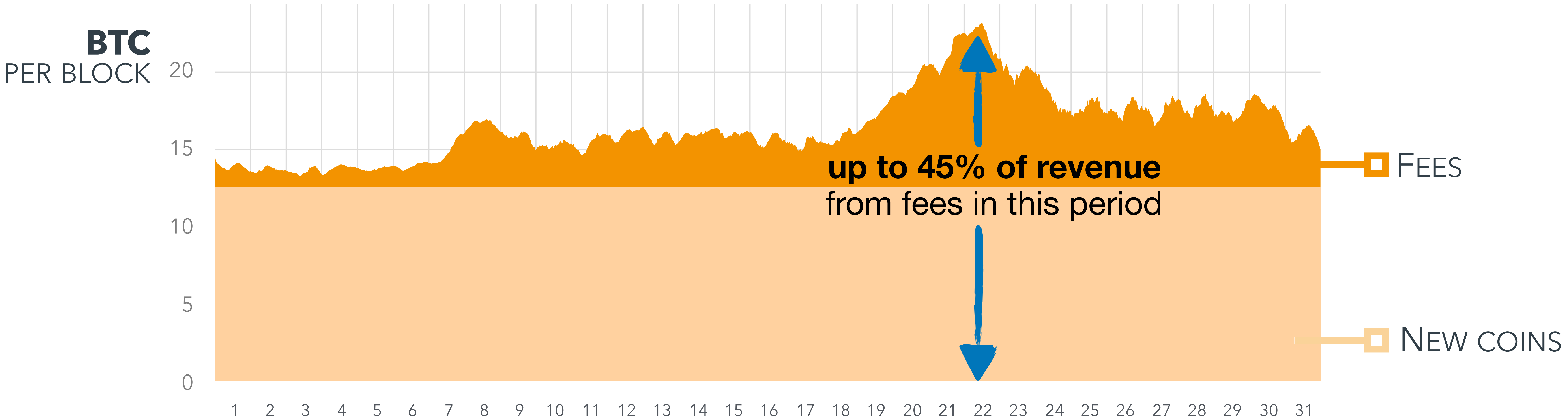
Mining revenues (2011-17)

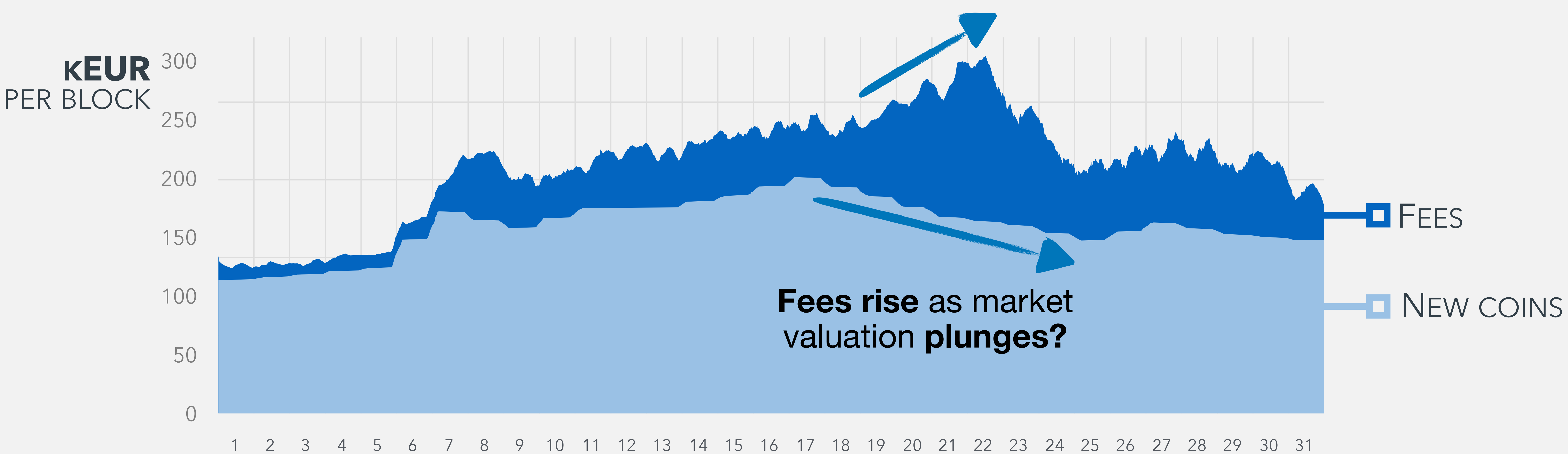


Mining **revenues** (2017)

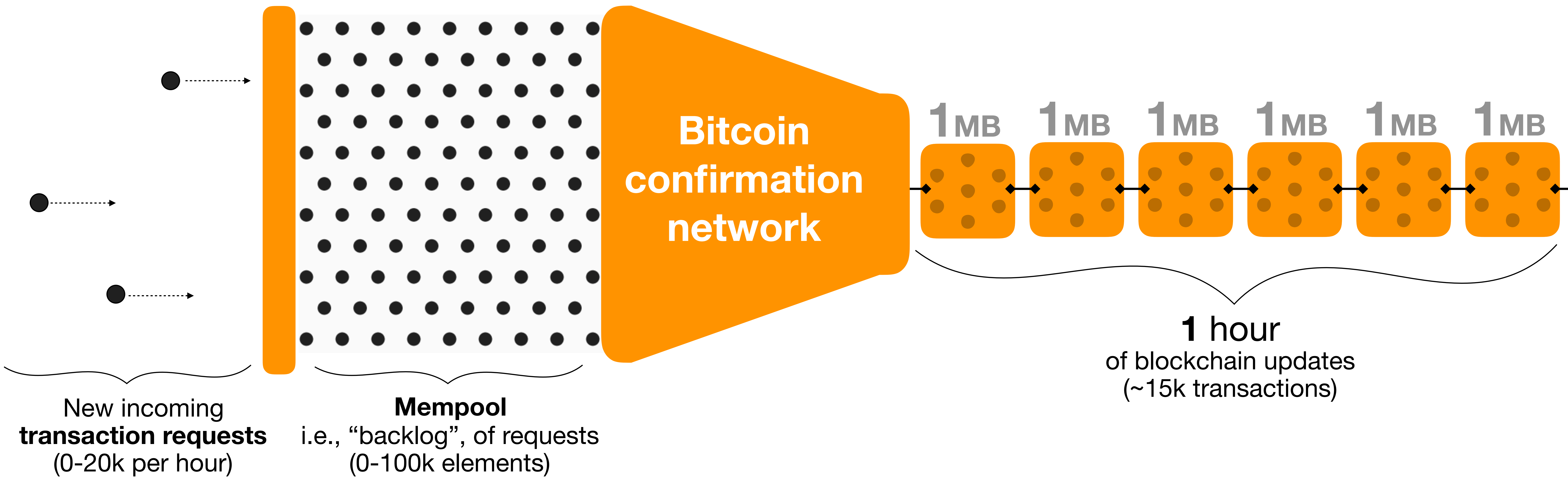


Mining **revenues** (dec. 2017)





Mechanics of
BTC confirmation



Unlike in traditional payment systems, in BTC…

- Confirmed volume per unit of time is a **scarce resource**:
  - No more than **6MB/hour** worth of transactions on avg.
- This ensues from two params **locked** at protocol level:
  - fixed block size (~1MB, i.e. 10^6 minus headers etc.)
  - controlled speed of block confirmation (every 10' on avg.)

Mechanics of
BTC confirmation

Unlike in traditional payment systems, in BTC…

- Confirmed volume per unit of time is a **scarce resource**:
  - No more than **6MB/hour** worth of transactions on avg.
- This ensues from two params **locked** at protocol level:
  - fixed block size (~1MB, i.e. 10^6 minus headers etc.)
  - controlled speed of block confirmation (every 10’ on avg.)

- The **fee** is **freely chosen** by the customer, tip-like, not by the “service providers” (miners);
- Dually, miners are free to **process or put on hold** transactions indefinitely, as they wish.

Economics of **BTC fees**

Unlike in traditional payment systems, in BTC…

- Confirmed volume per unit of time is a **scarce resource**:
  - No more than **6MB/hour** worth of transactions on avg.
- This ensues from two params **locked** at protocol level:
  - fixed block size (~1MB, i.e. 10^6 minus headers etc.)
  - controlled speed of block confirmation (every 10’ on avg.)

- The **fee** is **freely chosen** by the customer, tip-like, not by the “service providers” (miners);
- Dually, miners are free to **process or put on hold** transactions indefinitely, as they wish.

How does a **fluid market** adjust to these conditions?

What do Bitcoin **users** experience?

What does a “**rational miner**” do under these conditions?

Economics of **BTC fees**

Unlike in traditional payment systems, in BTC…

- Confirmed volume per unit of time is a **scarce resource**:
  - No more than **6MB/hour** worth of transactions on avg.
- This ensues from two params **locked** at protocol level:
  - fixed block size (~1MB, i.e. 10^6 minus headers etc.)
  - controlled speed of block confirmation (every 10' on avg.)

- The **fee** is **freely chosen** by the customer, tip-like, not by the "service providers" (miners);
- Dually, miners are free to **process or put on hold** transactions indefinitely, as they wish.

How does a **fluid market** adjust to these conditions?

(a) it reasons in terms of "*fee paid per byte occupied*" (whereas **the transacted amount plays little/no role**);

(b) fees rise **under large demand** of transactional capacity;

What do Bitcoin **users** experience?

(c) different "**QoS**" levels emerge for different fee "tiers";

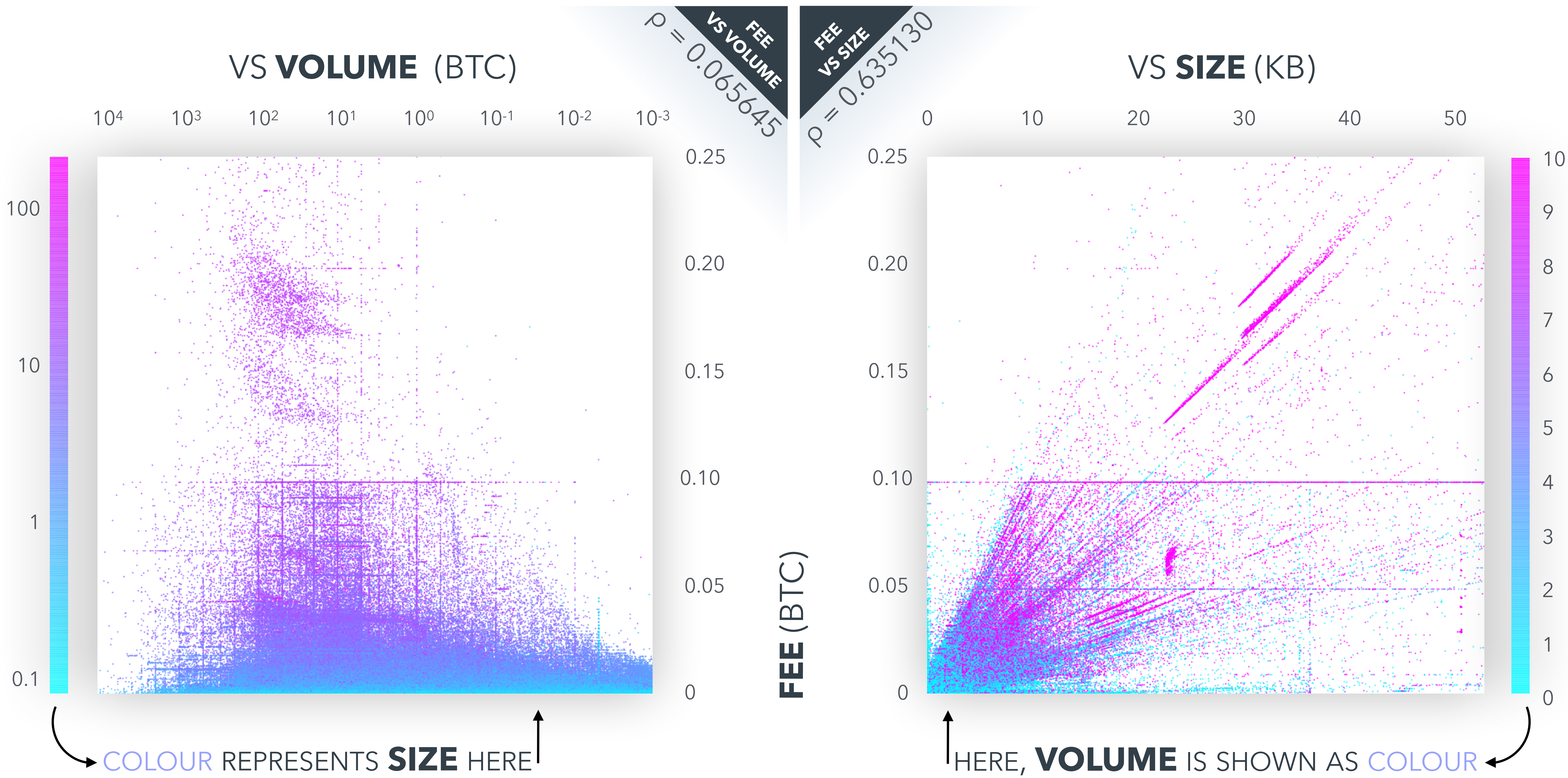
(d) fees get **too high** for some use cases;

What does a "**rational miner**" do under these conditions?

(e) tries to fill each block with the "**best**" transactions (new competition for fees **in addition to** block mining).

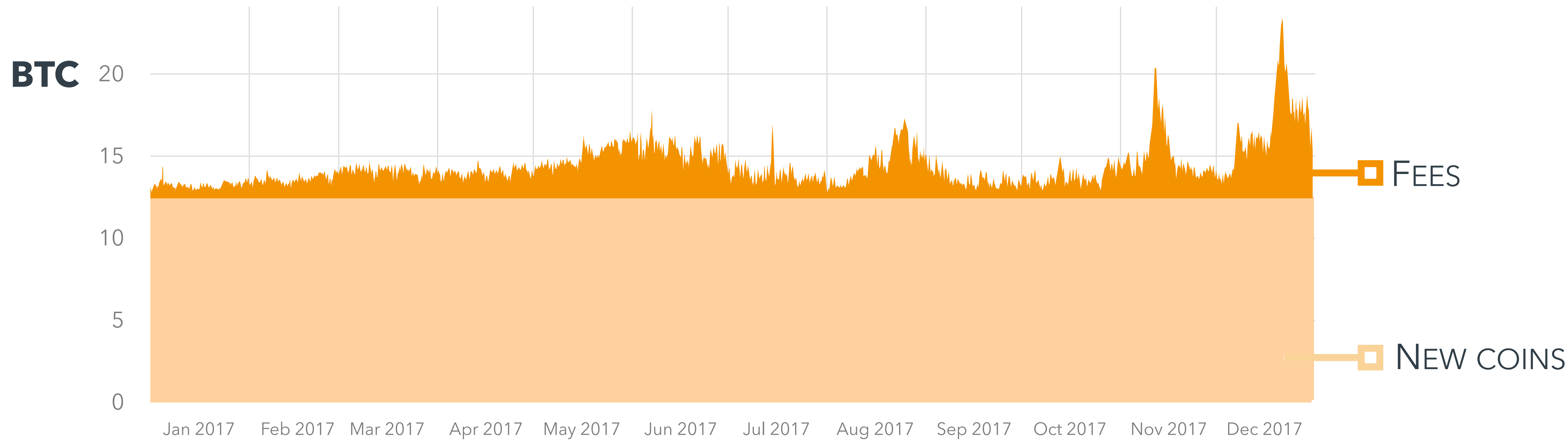
Fee VS **Size** VS **Volume** (a)

Does the market reason in terms of "*fee paid per byte occupied*"?
(whereas **the transacted amount plays little/no role**)

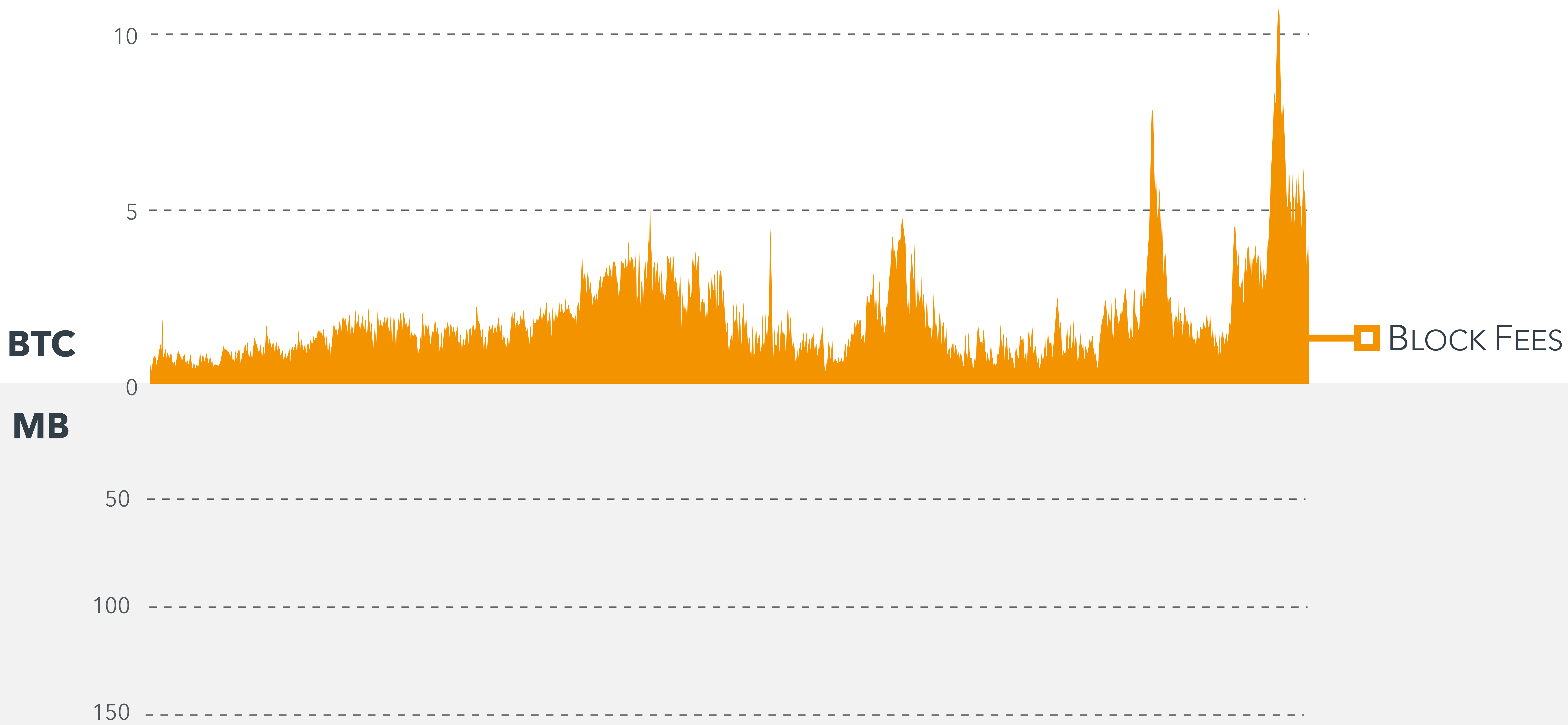


[Dec. 2017: **4.4k** blocks, **10.5M** transactions]

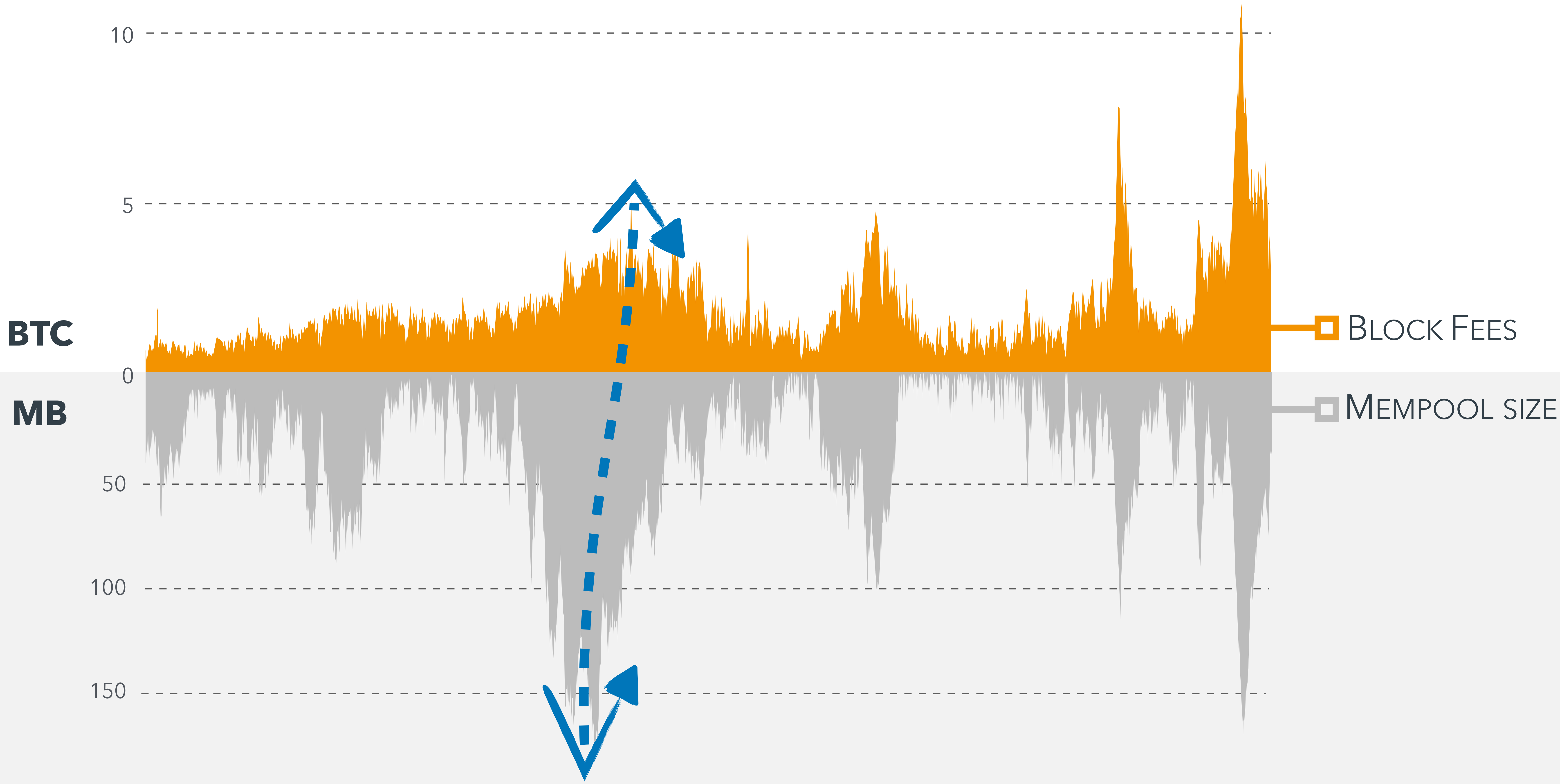
Mining **revenues** (2017) (b)



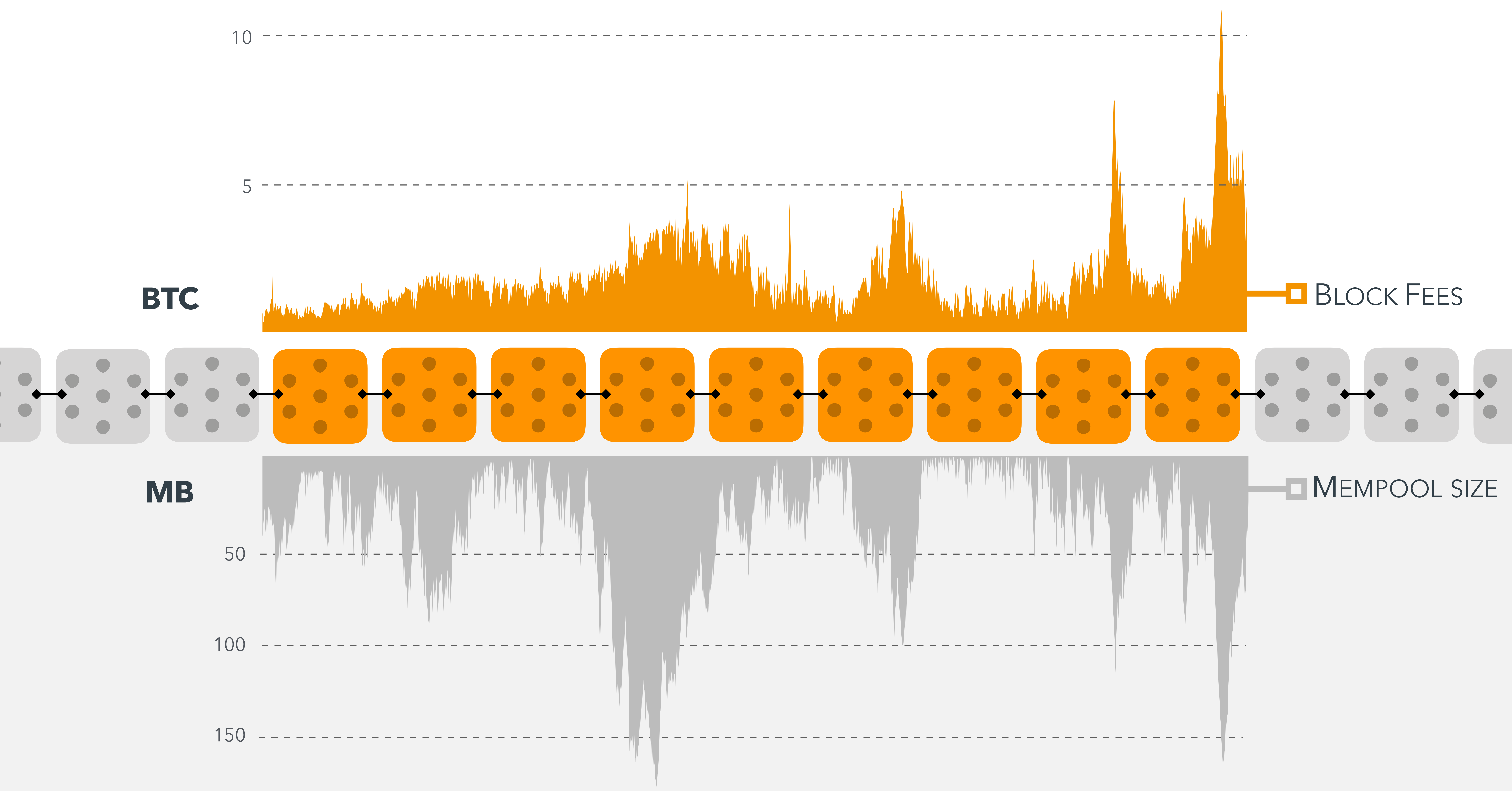
Mining **revenues** (2017) (b)



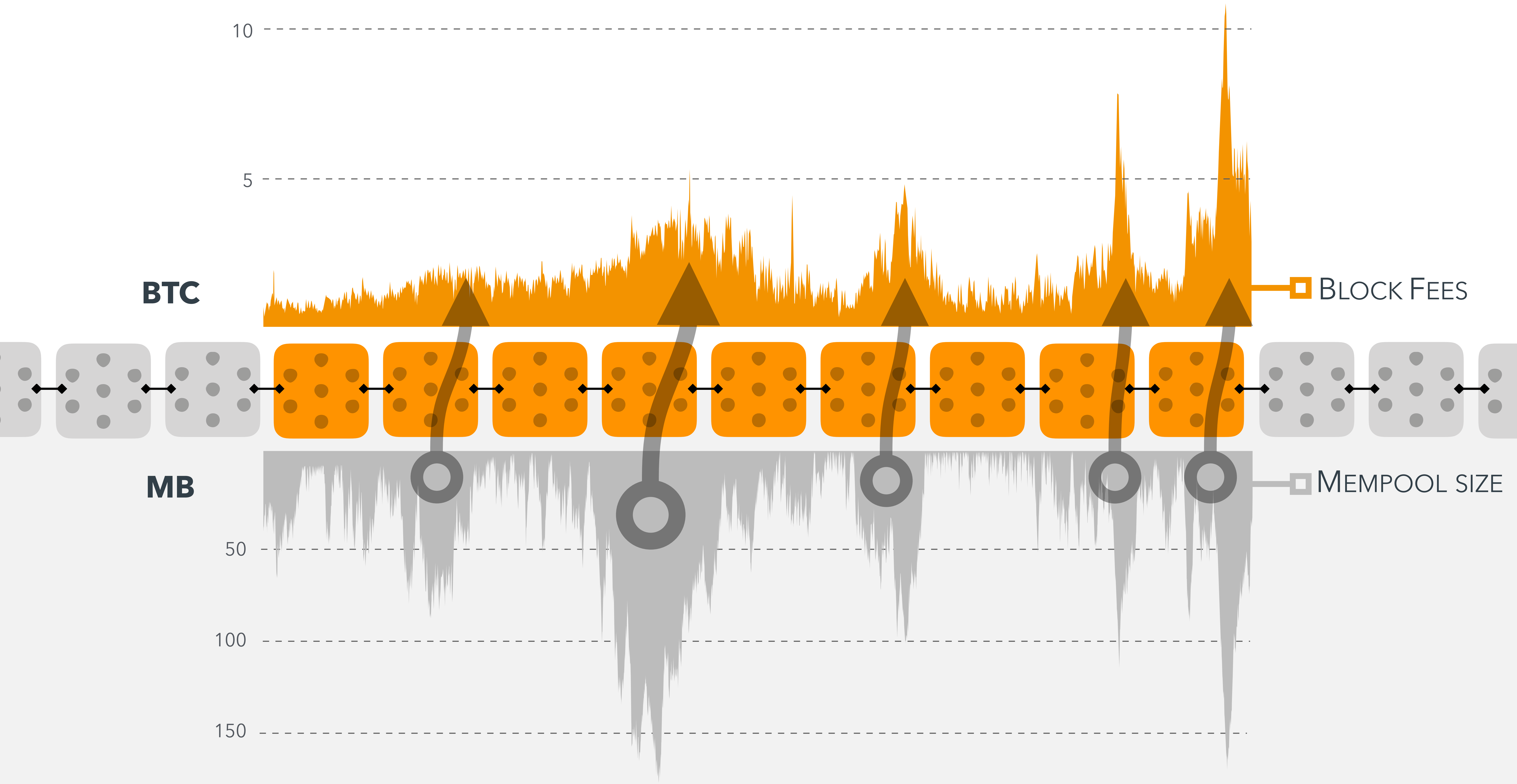
Mempool **size** VS block **fees** (b)



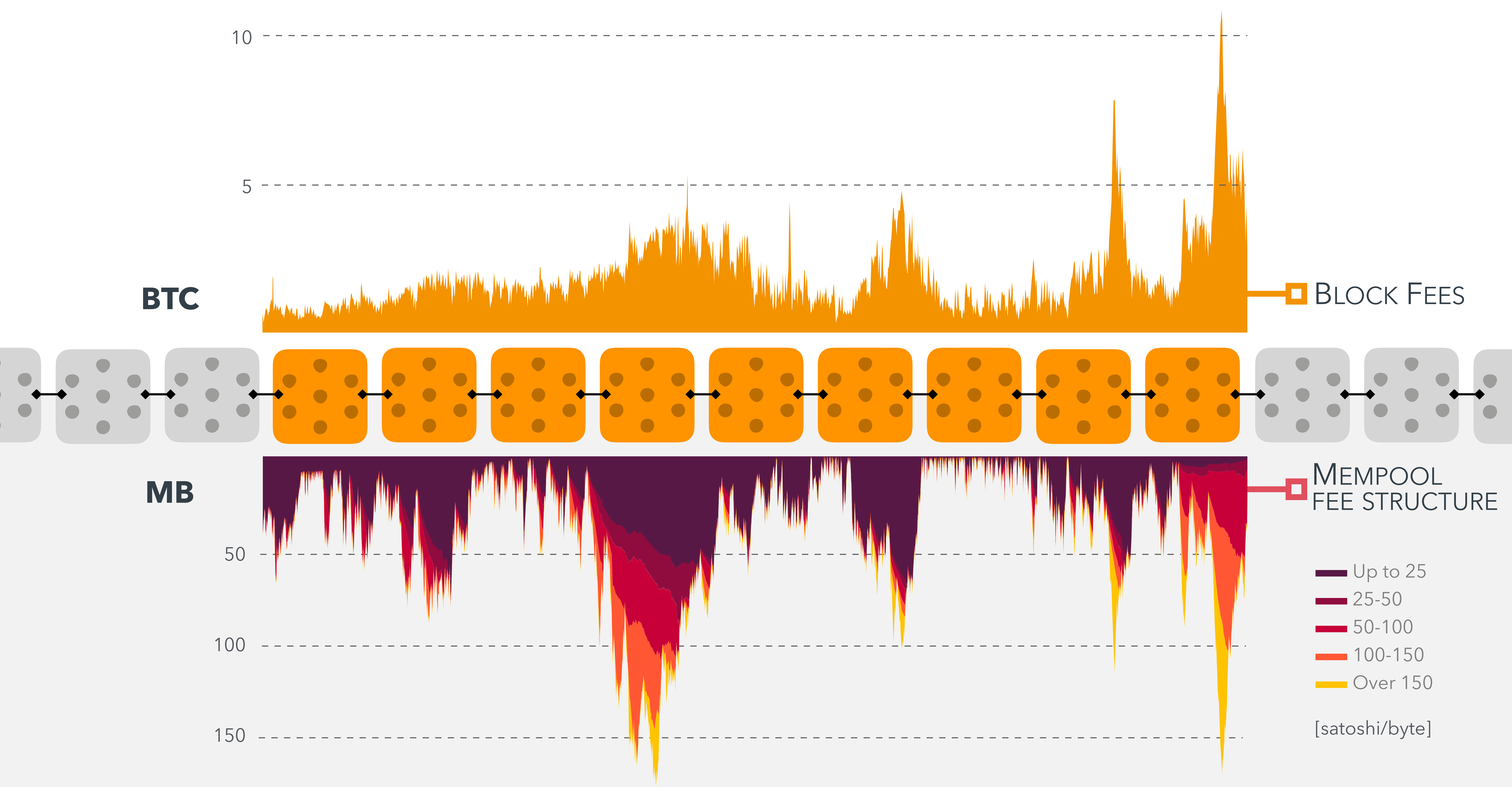
Mempool **size** VS block **fees** (b)



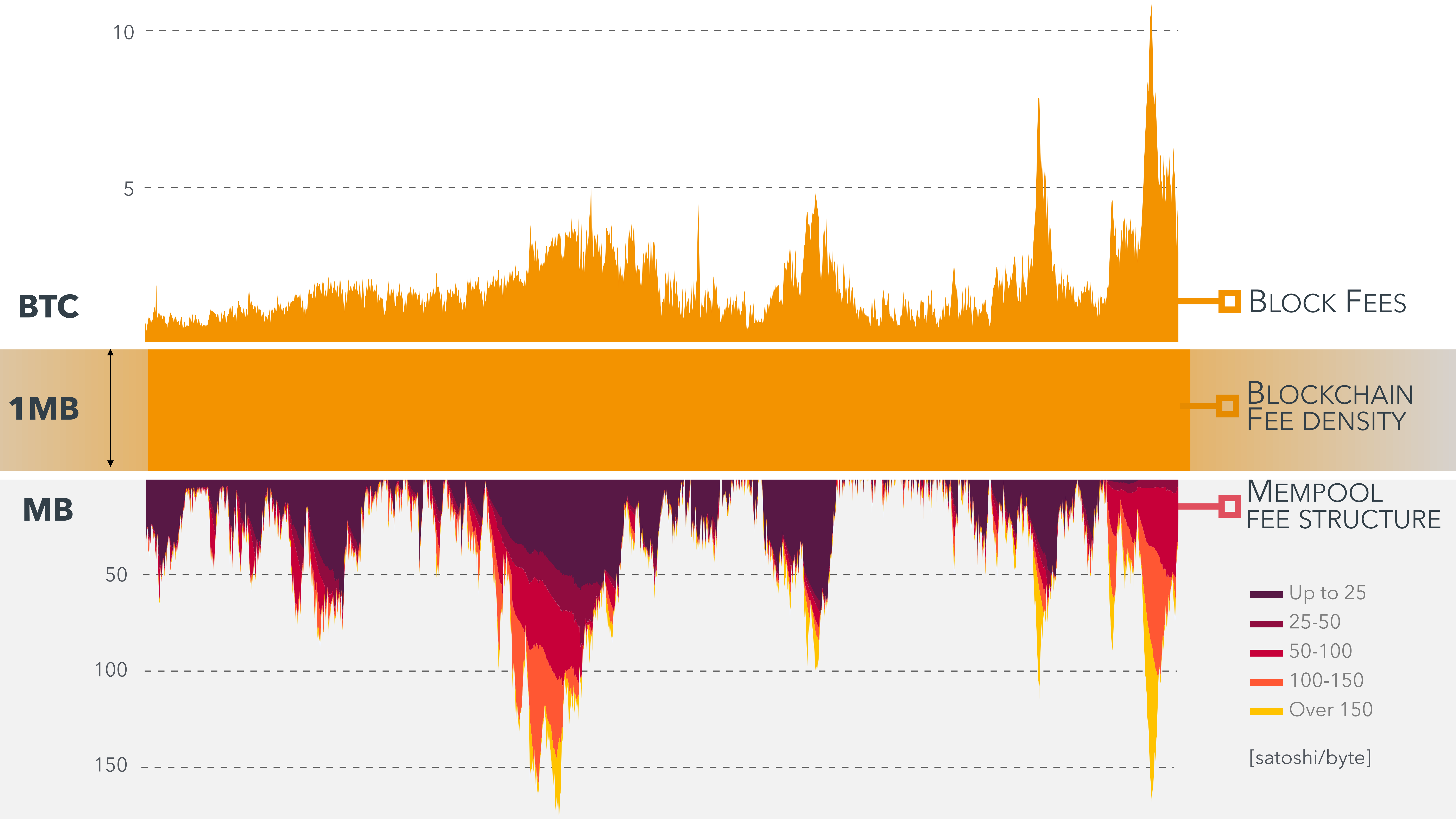
Mempool VS **fees** VS **Blockchain**(b)



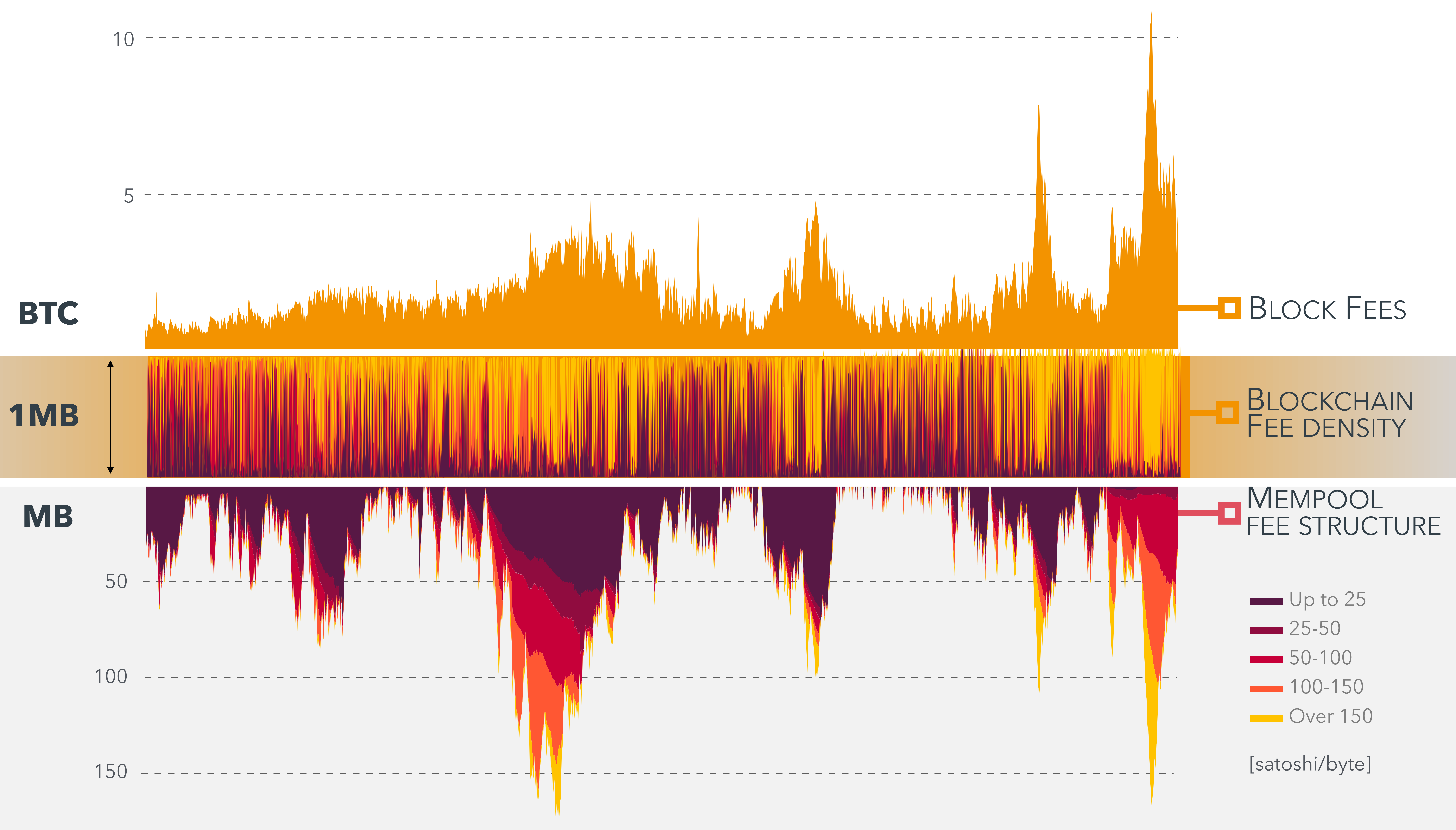
Mempool VS **fees** VS **Blockchain**(b)



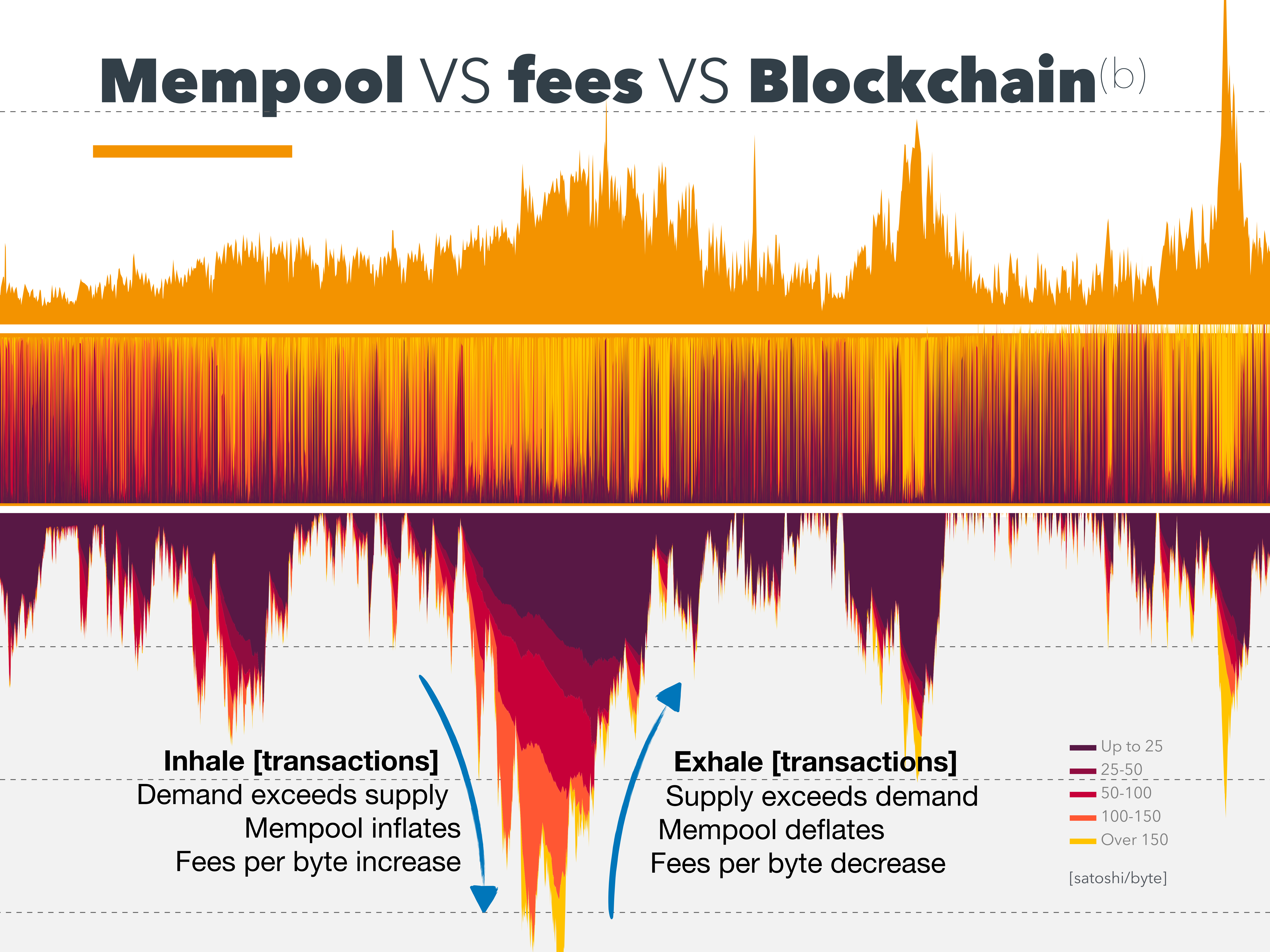
Mempool VS **fees** VS **Blockchain**(b)



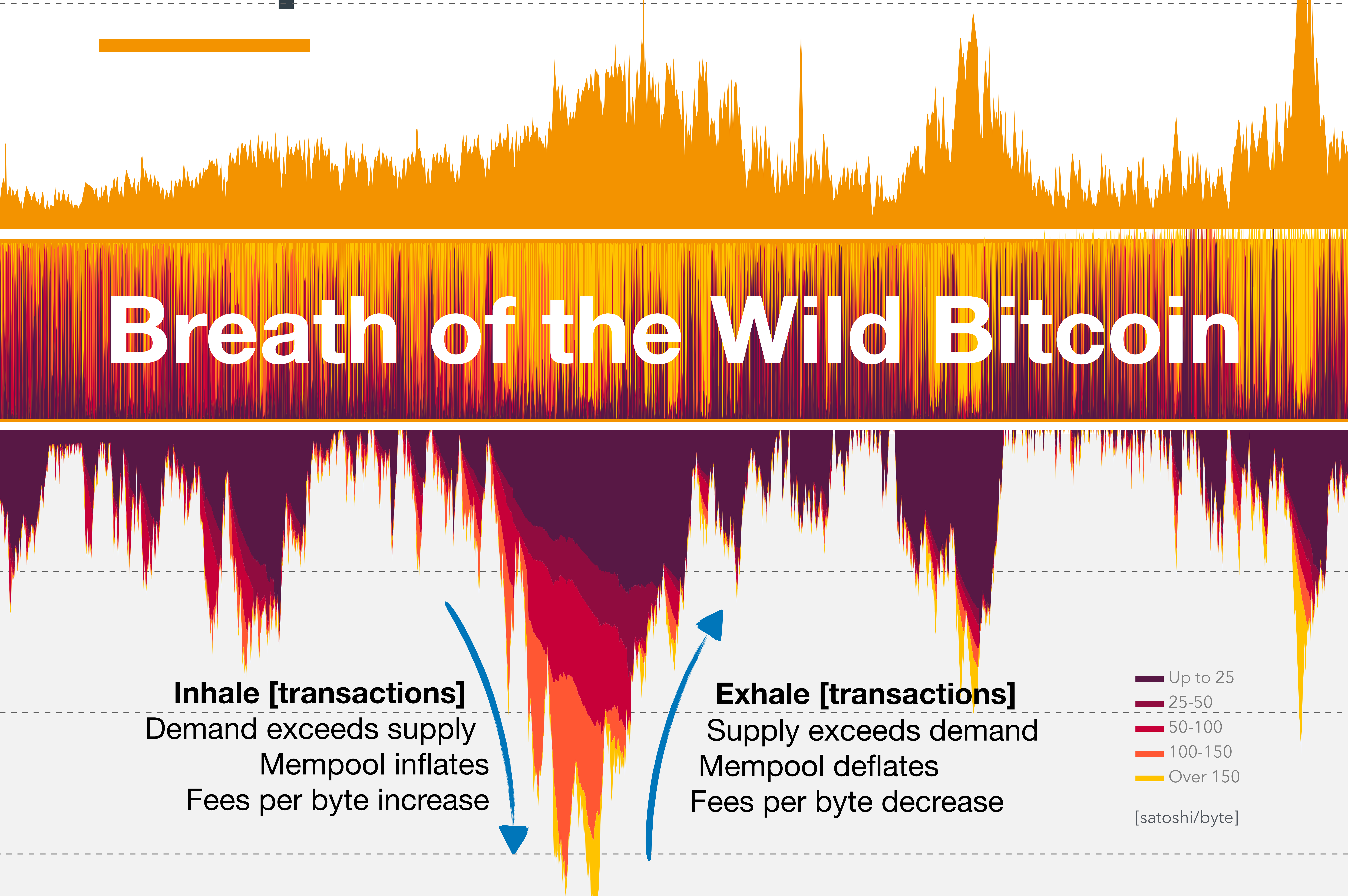
Mempool VS **fees** VS **Blockchain**(b)



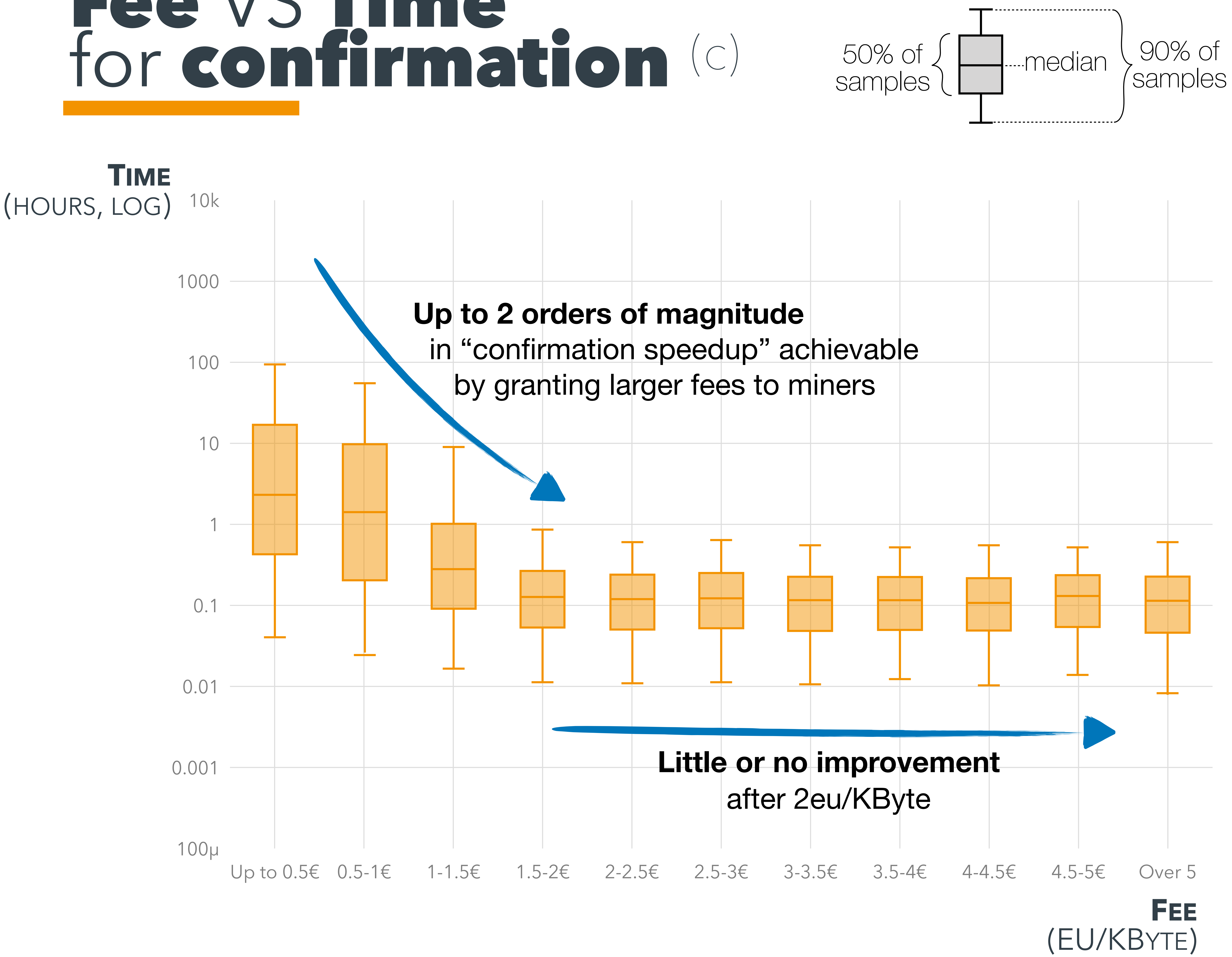
Mempool VS **fees** VS **Blockchain**(b)



Mempool VS **fees** VS **Blockchain**(b)



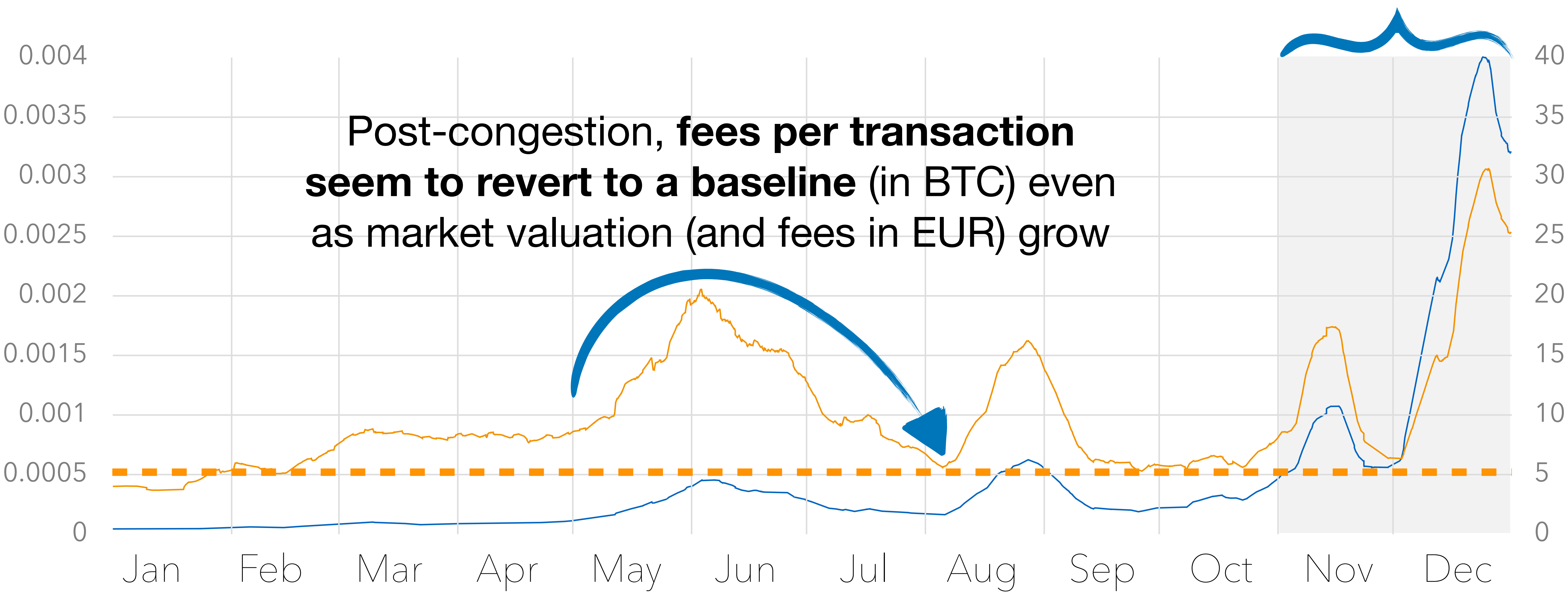
Fee VS **Time** for **confirmation** (c)



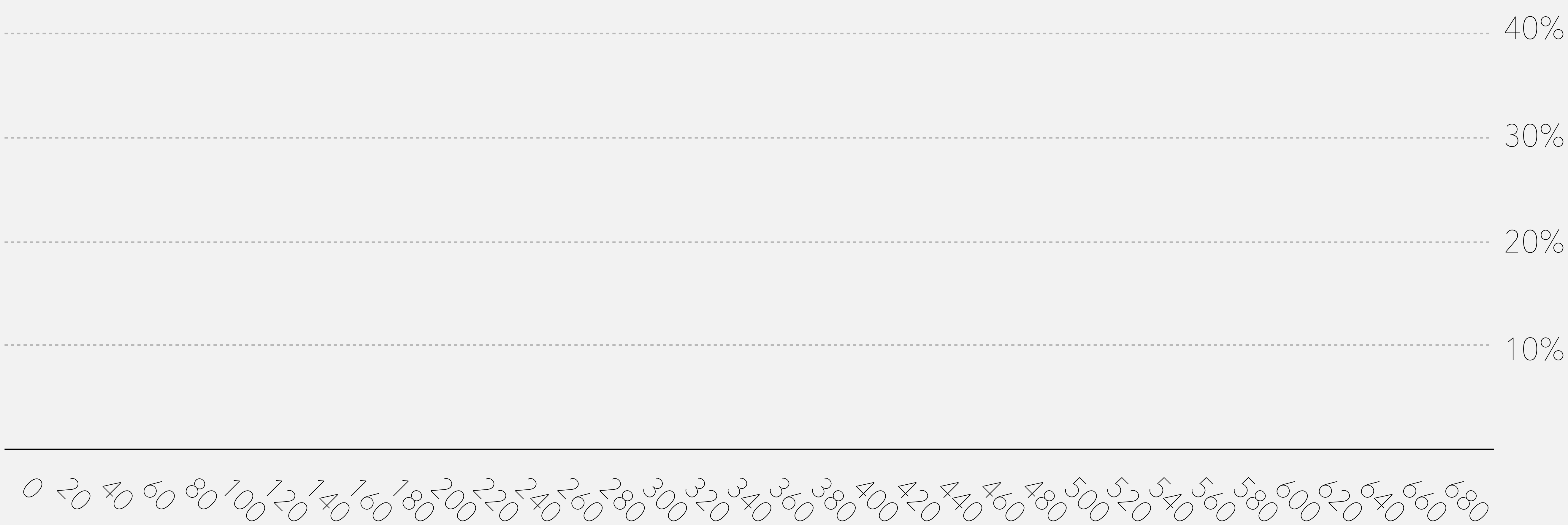
[Random sample of **250k** transactions sent & confirmed during April 2017]

Fee **amount** and **distribution [2017]** (d)

Fees may suddenly become too high (>5eu/tr) for many common use cases (e.g., retail payments)



AVERAGE FEE
PER TRANSACTION
IN BTC AND EUR

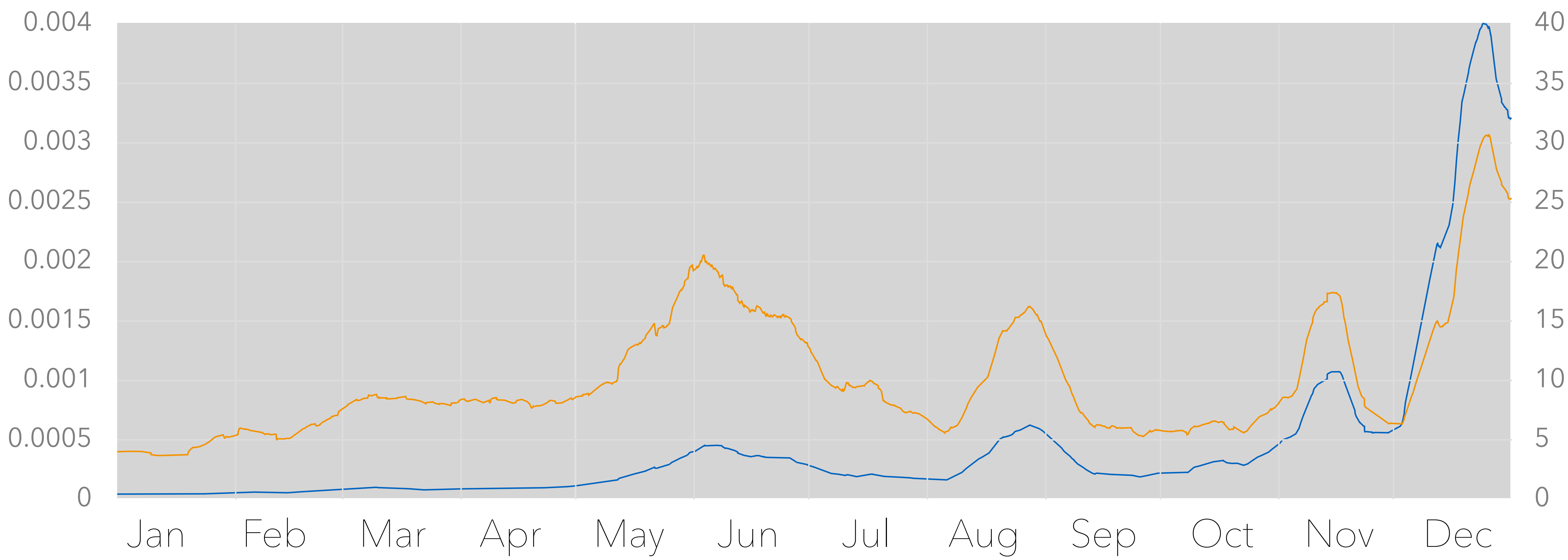


PERCENTAGE
OF TRANSACTIONS WITH A GIVEN FEE

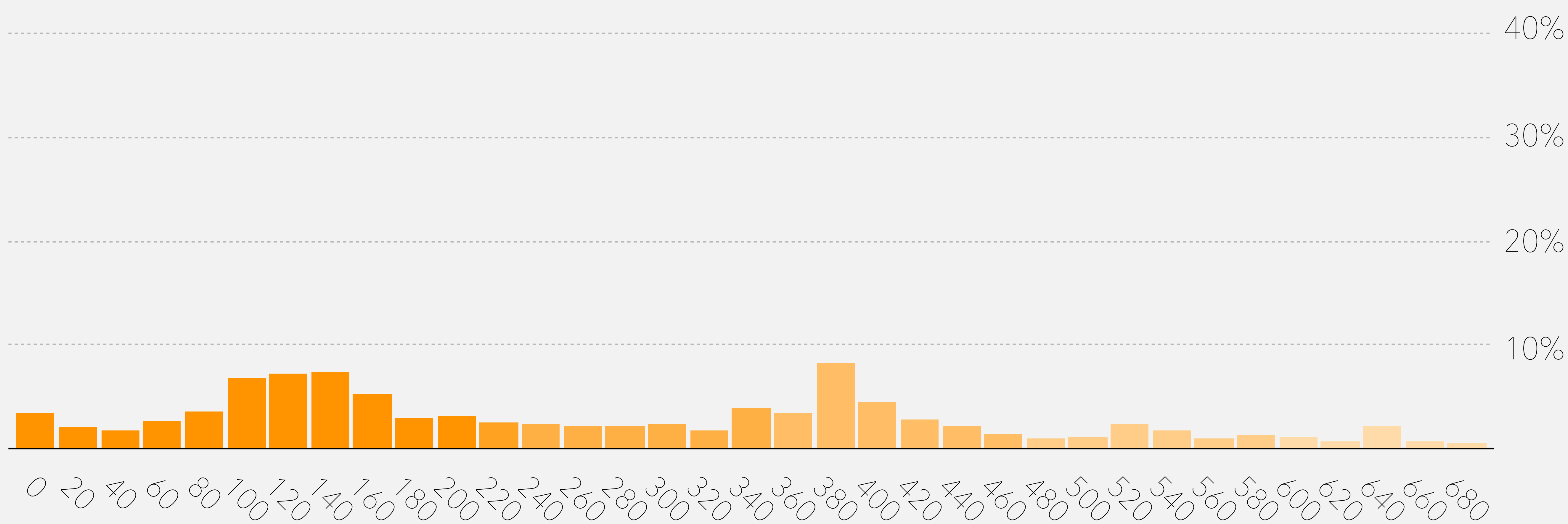
SATOSHI/BYTE

(WEIGHTED BY SIZE)

Fee **amount** and **distribution [2017]** (d)



AVERAGE FEE
PER TRANSACTION
IN BTC AND EUR



PERCENTAGE
OF TRANSACTIONS
WITH A GIVEN FEE

SATOSHI/BYTE

(WEIGHTED BY SIZE)

Mining as an **optimisation problem** (e)

Given n transactions with fees $v_1, \ldots, v_n$ (satoshi) and size $w_1, \ldots, w_n$ (bytes), let C be the capacity of the block (in bytes); then, decide whether the i-th transaction should be included ($x_i = 1$) or not ($x_i = 0$) in so as to:

$$\texttt{maximize} \quad \sum_{i=1}^{n} x_i \cdot v_i$$

$$\texttt{subject to} \quad \sum_{i=1}^{n} x_i \cdot w_i \leq C$$

Mining as an **optimisation problem** (e)

Given n transactions with fees $v_1, \ldots, v_n$ (satoshi) and size $w_1, \ldots, w_n$ (bytes), let C be the capacity of the block (in bytes); then, decide whether the i-th transaction should be included ($x_i = 1$) or not ($x_i = 0$) in so as to:

$$\texttt{maximize} \quad \sum_{i=1}^{n} x_i \cdot v_i$$

$$\texttt{subject to} \quad \sum_{i=1}^{n} x_i \cdot w_i \leq C$$

Let's make the **best possible use** of the limited resource (space) available

0-1 Knapsack problem

Mining as an **optimisation problem** (e)

Given n transactions with fees $v_1, \ldots, v_n$ (satoshi) and size $w_1, \ldots, w_n$ (bytes), let C be the capacity of the block (in bytes); then, decide whether the i-th transaction should be included ($x_i = 1$) or not ($x_i = 0$) in so as to:

$$\texttt{maximize} \quad \sum_{i=1}^{n} x_i \cdot v_i$$

$$\texttt{subject to} \quad \sum_{i=1}^{n} x_i \cdot w_i \leq C$$

Let's make the **best possible use** of the limited resource (space) available

0-1 Knapsack problem

$$\texttt{subject to} \quad x_i \leq x_j \ \forall (i,j) \in E$$

Don't include transactions that miss any **causal preconditions**; E is a transitive relation

Precedence constrained

Mining as an **optimisation problem** (e)

Given n transactions with fees $v_1, \ldots, v_n$ (satoshi) and size $w_1, \ldots, w_n$ (bytes), let C be the capacity of the block (in bytes); then, decide whether the i-th transaction should be included ($x_i = 1$) or not ($x_i = 0$) in so as to:

$$\texttt{maximize} \quad \sum_{i=1}^{n} x_i \cdot v_i$$

$$\texttt{subject to} \quad \sum_{i=1}^{n} x_i \cdot w_i \leq C$$

Let's make the **best possible use** of the limited resource (space) available

0-1 Knapsack problem

$$\texttt{subject to} \quad x_i \leq x_j \; \forall (i,j) \in E$$

Don't include transactions that miss any **causal preconditions**; E is a transitive relation

Precedence constrained

Mining as an **optimisation problem** (e)

Given n transactions with fees $v_1, \ldots, v_n$ (satoshi) and size $w_1, \ldots, w_n$ (bytes), let C be the capacity of the block (in bytes); then, decide whether the i-th transaction should be included ($x_i = 1$) or not ($x_i = 0$) in so as to:

$$\texttt{maximize} \sum_{i=1}^{n} x_i \cdot v_i$$

$$\texttt{subject to} \sum_{i=1}^{n} x_i \cdot w_i \leq C$$

Let's make the **best possible use** of the limited resource (space) available

0-1 Knapsack problem

$$\texttt{subject to } x_i \leq x_j \; \forall (i,j) \in E$$

Don't include transactions that miss any **causal preconditions**; E is a transitive relation

Precedence constrained

$$\texttt{subject to } x_i + x_j \leq 1 \; \forall (i,j) \in D$$

Filter-out **double spending**; D contains all couples of mutually inconsistent transactions

Maximum independent set problem

Mining as an **optimisation problem** (e)

Given n transactions with fees $v_1, \ldots, v_n$ (satoshi) and size $w_1, \ldots, w_n$ (bytes), let C be the capacity of the block (in bytes); then, decide whether the i-th transaction should be included ($x_i = 1$) or not ($x_i = 0$) in so as to:

$\texttt{maximize} \sum_{i=1}^{n} x_i \cdot v_i$ $\texttt{subject to} \sum_{i=1}^{n} x_i \cdot w_i \leq C$	Let's make the **best possible use** of the limited resource (space) available	**0-1 Knapsack problem**
$\texttt{subject to } x_i \leq x_j \ \forall (i,j) \in E$	Don't include transactions that miss any **causal preconditions**; E is a transitive relation	**Precedence constrained**
$\texttt{subject to } x_i + x_j \leq 1 \ \forall (i,j) \in D$	Filter-out **double spending**; D contains all couples of mutually inconsistent transactions	**Maximum independent set problem**
$(w_{n+1}, v_{n+1}), (w_{n+2}, v_{n+2}), \ldots$	New transactions arrive and have to be taken into account **on the fly**	**Online, multi-period**

Mining as an **optimisation problem** (e)

Given n transactions with fees $v_1, \ldots, v_n$ (satoshi) and size $w_1, \ldots, w_n$ (bytes), let C be the capacity of the block (in bytes); then, decide whether the i-th transaction should be included ($x_i = 1$) or not ($x_i = 0$) in so as to:

$$\texttt{maximize} \sum_{i=1}^{n} x_i \cdot v_i$$

Known to be **NP-Hard.** Some variants have (F)PTAS. Tractable **in practice**?

☞ Difficult in practice, too. Typical instance is like this: n≃50k objects, w_i in 100-100k, v_i in 0-10M, C≃1000k

$$\texttt{subject to} \sum_{i=1}^{n} x_i \cdot w_i \leq C$$

$$\texttt{subject to}\ x_i \leq x_j\ \forall (i,j) \in E$$

Is this **uncommon**?

☞ Our analysis shows it **isn't**; strongly precedence-constrained instances

---

$$\texttt{subject to}\ x_i + x_j \leq 1\ \forall (i,j) \in D$$

Is this **infrequent**?

☞ **Yes**; policy applied by nodes neutralises this case

$$(w_{n+1}, v_{n+1}), (w_{n+2}, v_{n+2}), \ldots$$

Is this **negligible**?

☞ **No**: 1,860 new transactions arrive (avg) to miners in the time it takes (avg) to confirm a block [2017 values]

Mining as an **optimisation problem** (e)

Given n transactions with fees $v_1, \ldots, v_n$ (satoshi) and size $w_1, \ldots, w_n$ (bytes), let C be the capacity of the block (in bytes); then, decide whether the i-th transaction should be included ($x_i = 1$) or not ($x_i = 0$) in so as to:

$$\texttt{maximize} \sum_{i=1}^{n} x_i \cdot v_i$$

$$\texttt{subject to} \sum_{i=1}^{n} x_i \cdot w_i \leq C$$

$$\texttt{subject to}\ x_i \leq x_j\ \forall (i,j) \in E$$

Known to be **NP-Hard.** Some variants have (F)PTAS. Tractable **in practice**?

☞ Difficult in practice, too. Typical instance is like this: n≃50k objects, w_i in 100-100k, v_i in 0-10M, C≃1000k

Is this **uncommon**?

☞ Our analysis shows it **isn't**; strongly precedence-constrained instances

---

$$\texttt{subject to}\ x_i + x_j \leq 1\ \forall (i,j) \in D$$

Is this **infrequent**?

☞ **Yes**; policy applied by nodes neutralises this case

$$(w_{n+1}, v_{n+1}), (w_{n+2}, v_{n+2}), \ldots$$

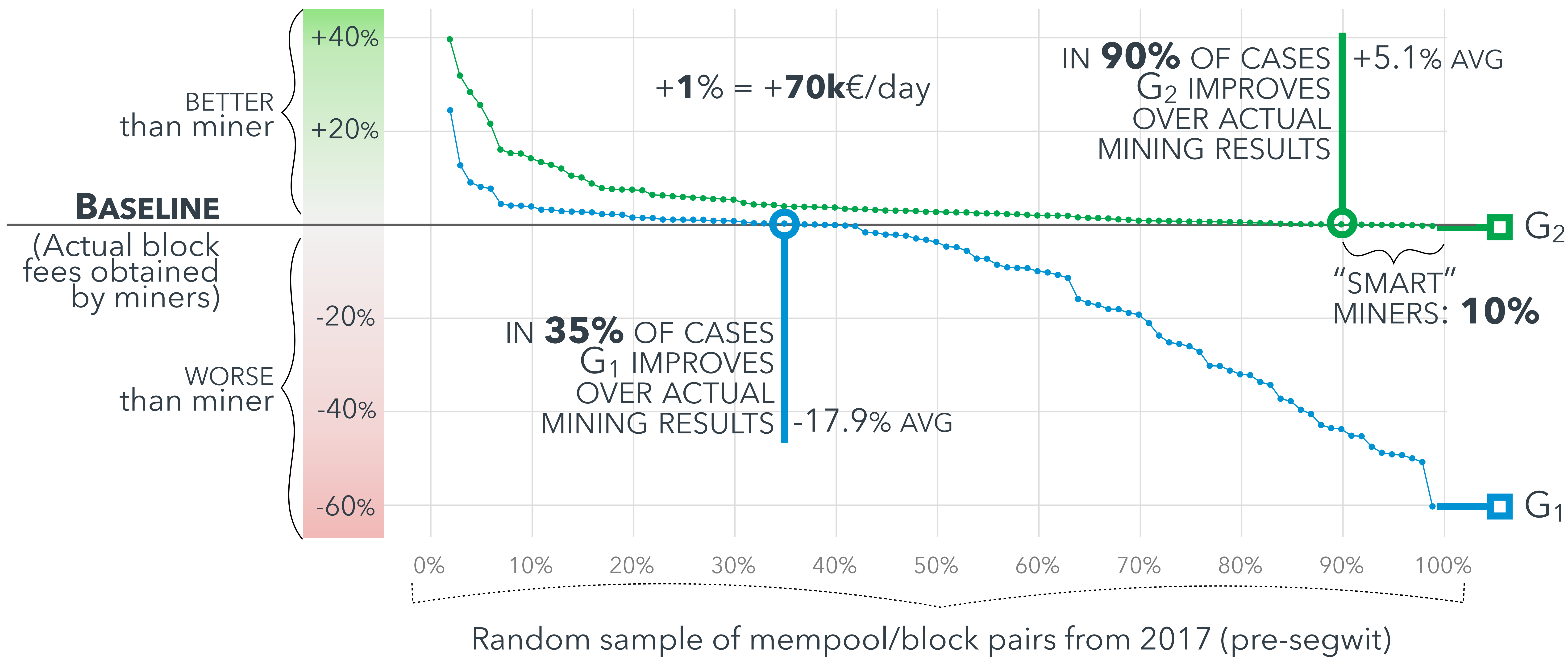
Is this **negligible**?

☞ **No**: 1,860 new transactions arrive (avg) to miners in the time it takes (avg) to confirm a block [2017 values]

Mining as an **optimisation problem** (e)

Given n transactions with fees $v_1, \ldots, v_n$ (satoshi) and size $w_1, \ldots, w_n$ (bytes), let C be the capacity of the block (in bytes); then, decide whether the i-th transaction should be included ($x_i = 1$) or not ($x_i = 0$) in so as to:

$$\texttt{maximize} \sum_{i=1}^{n} x_i \cdot v_i \qquad \texttt{subject to} \sum_{i=1}^{n} x_i \cdot w_i \leq C \qquad x_i \leq x_j \ \forall (i,j) \in E$$



Distributed Ledger Technology Workshop

1° febbraio 2018 Università degli Studi di Perugia

Blocks and **Fees** in **Bitcoin**

[Observationally Speaking]

Marco **Benedetti**, Gennaro **Catapano**, Francesco **De Sclavis***, Roberto **Favaroni**, Giuseppe **Galano**, Andrea **Gentili**, Marco **Mori**

[NAME].[SURNAME]@bancaditalia.it

ART www.bankit.art

*Intern at ART

BANCA D'ITALIA
EUROSISTEMA

The **opinions** expressed and conclusions drawn are those of the **authors** and do **not** necessarily reflect the views of the **Bank of Italy**.

Thank you for your attention

Any questions?

BANCA D'ITALIA
EUROSISTEMA

The **opinions** expressed and conclusions drawn are those of the **authors** and do **not** necessarily reflect the views of the **Bank of Italy**.