FlareSystems

Smart darknet intelligence for teams

Qui nous sommes

Mathieu Lavoie
CEO

Experience as a security team leader at Desjardins.
Bachelor in Information Technology eng.

Israël Hallé
CTO

Experience as software engineer and malware analyst at Shopify, Google.
Bachelor in software eng.

David Décary-Hétu
CSO

PhD in criminology, cybercrime and online illicit markets researcher

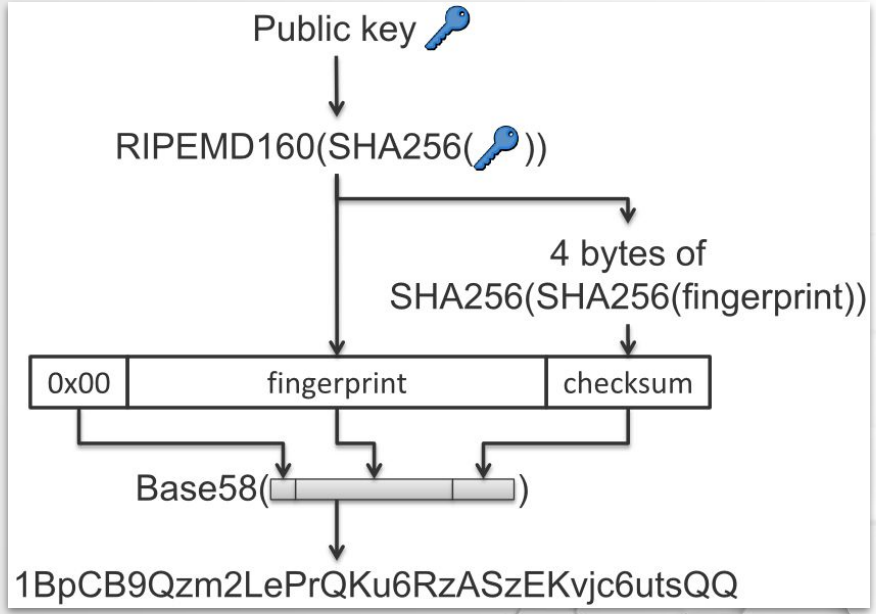
Au menu

- Bitcoin 101
- Les limites du pseudo-anonymat
- BitCluster

BITCOIN 101

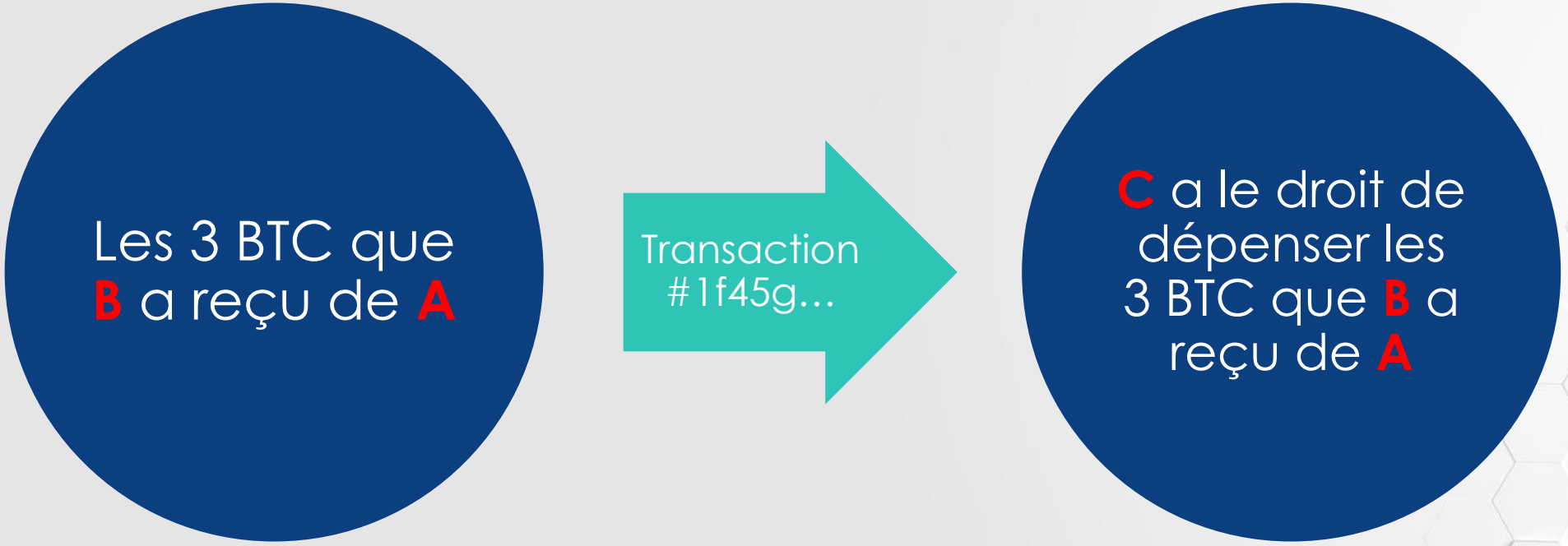
Adresses Bitcoin

- Représentation simplifiée d'une clé publique
- Génération par n'importe quel individu



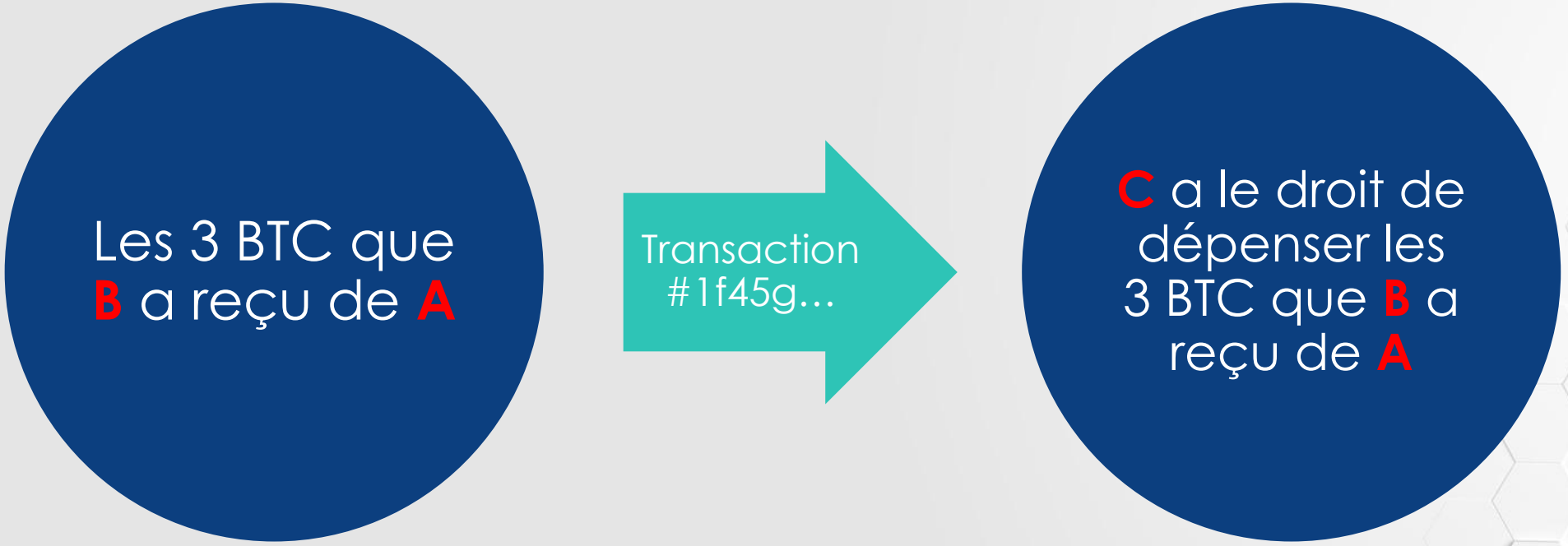
FlareSystems

Transactions

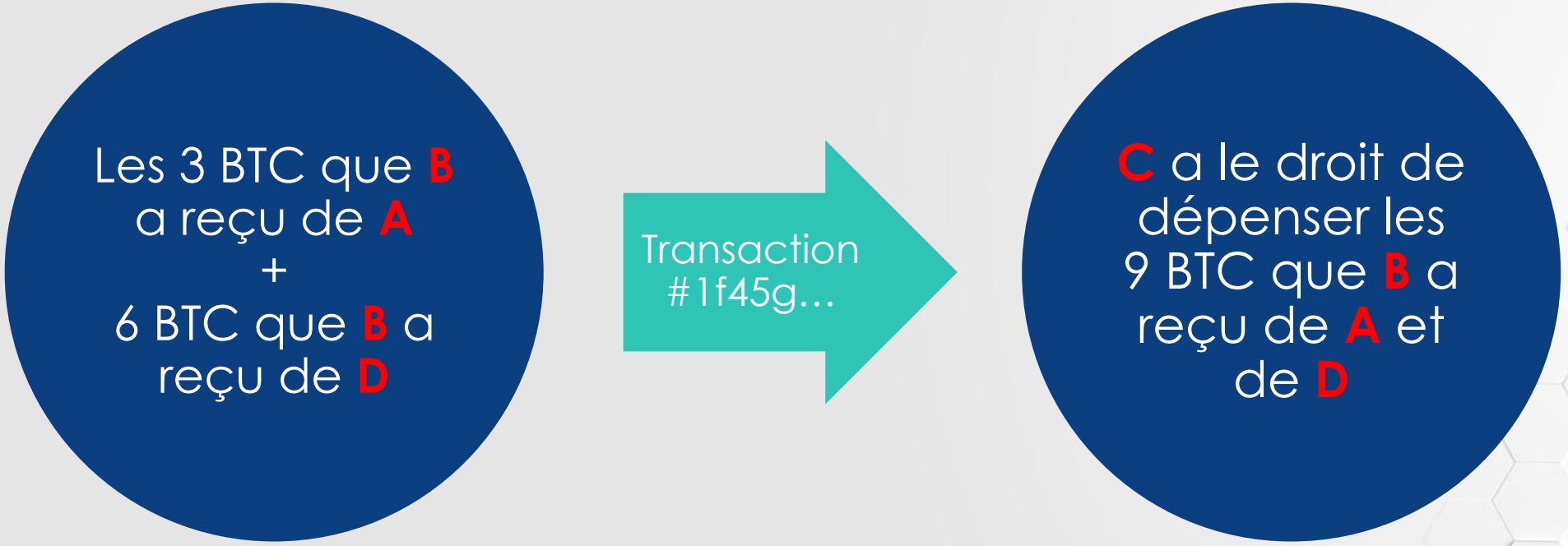


LES LIMITES DU PSEUDO-ANONYMAT

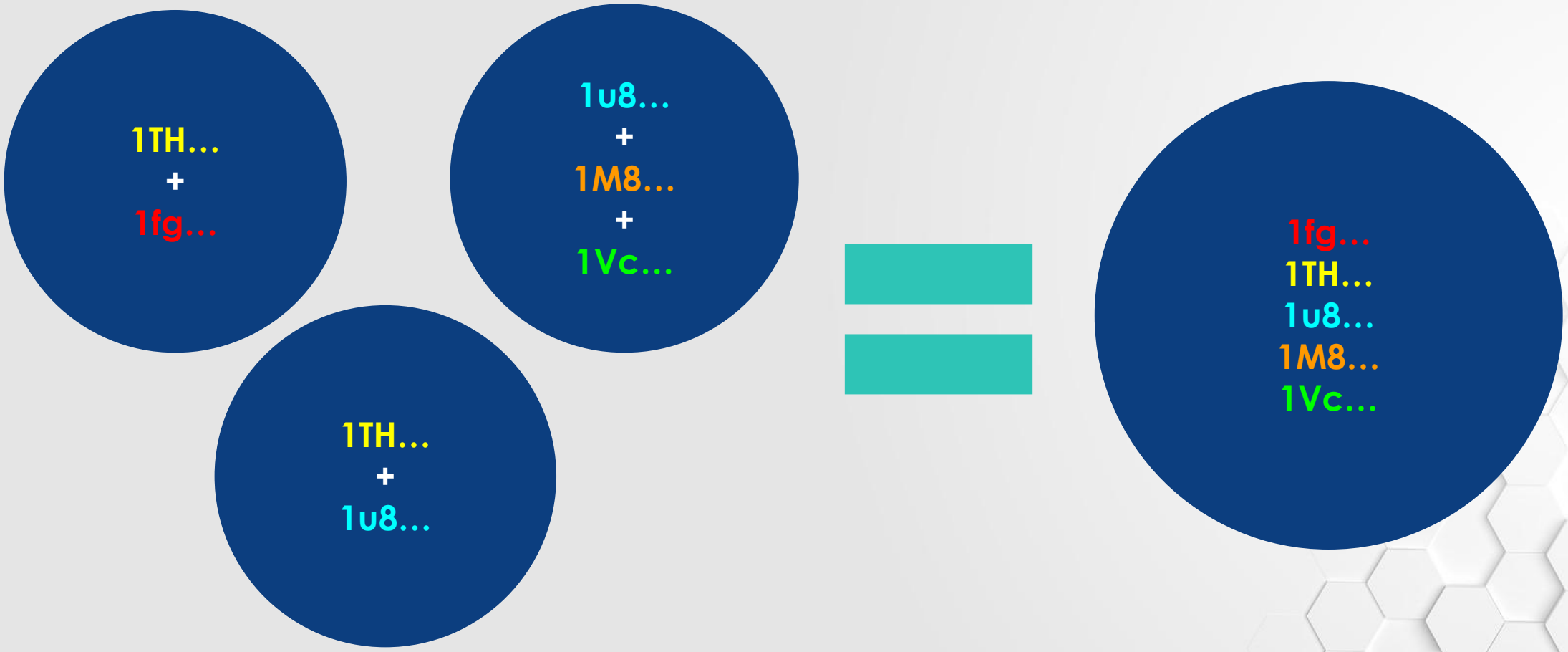
Transactions



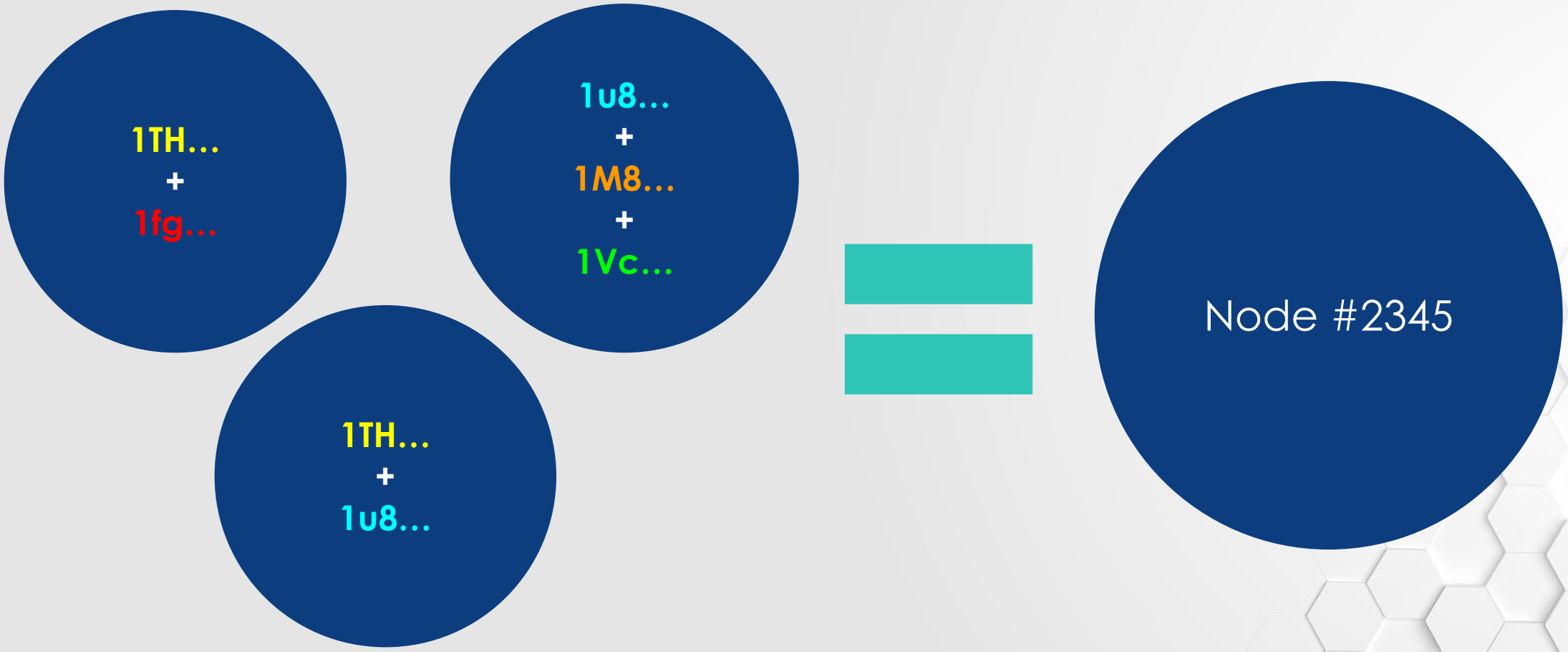
Transactions à plusieurs entrants



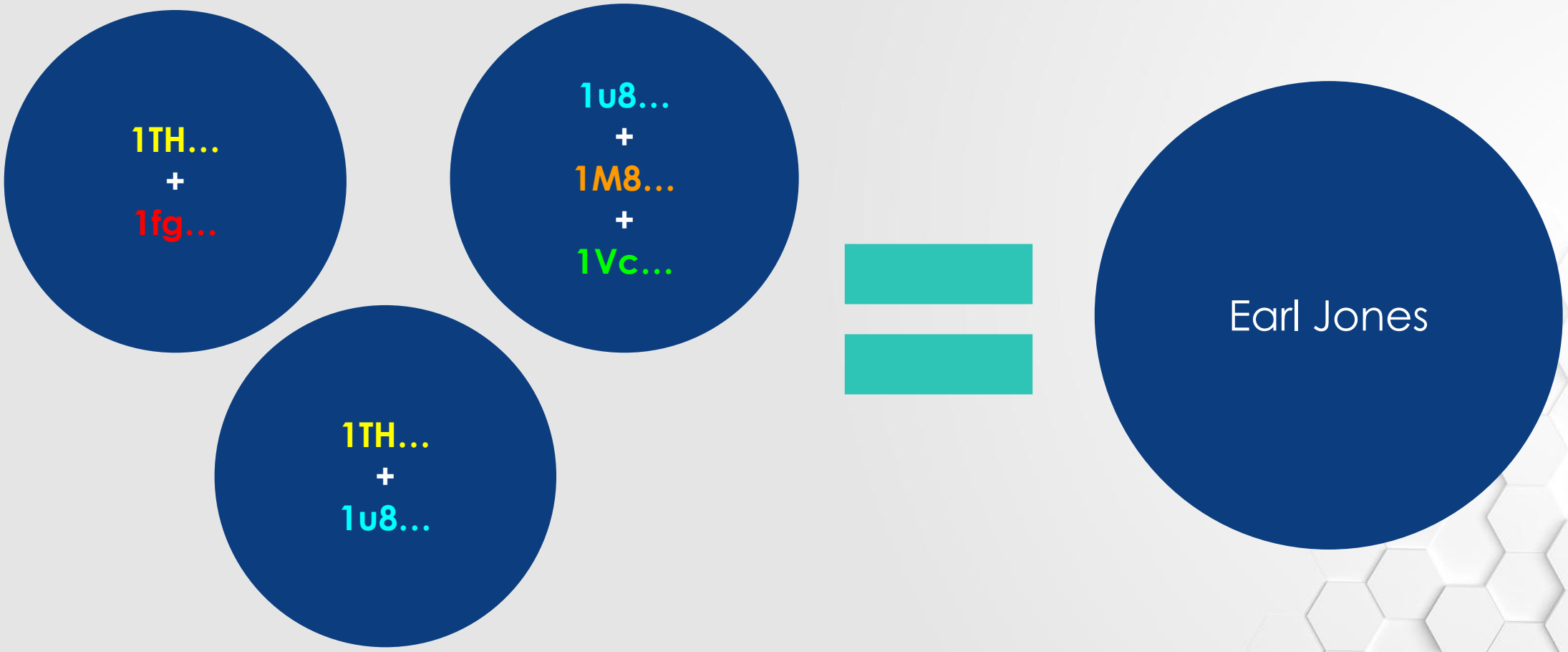
Transactions à plusieurs entrants
L'agrégation



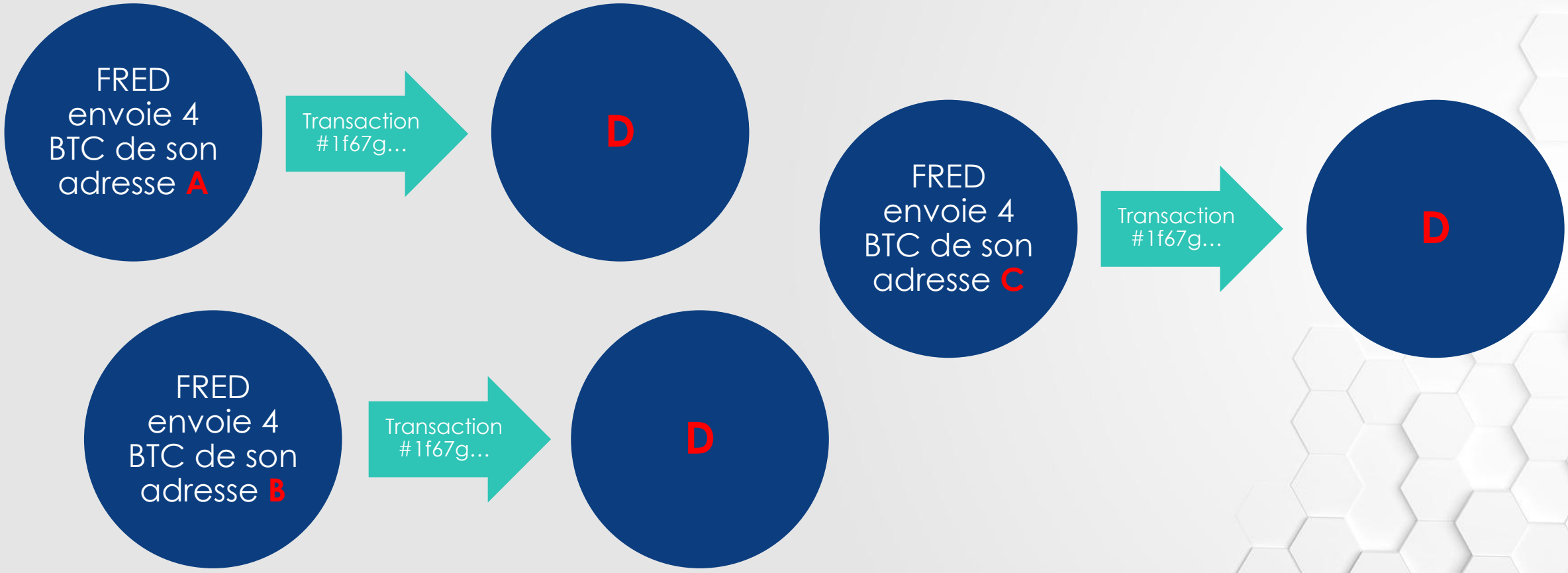
Transactions à plusieurs entrants
L'agrégation



Transactions à plusieurs entrants
L'agrégation



Rester anonyme



Hypothèses de départ

- Les transactions sont signées avec des clés privées
- Les clés privées sont… privées
- Une seule entité a accès à chaque clé privée
- Ergo une entité contrôle tous les wallets d'une transaction à plusieurs entrants

Déanonymisation

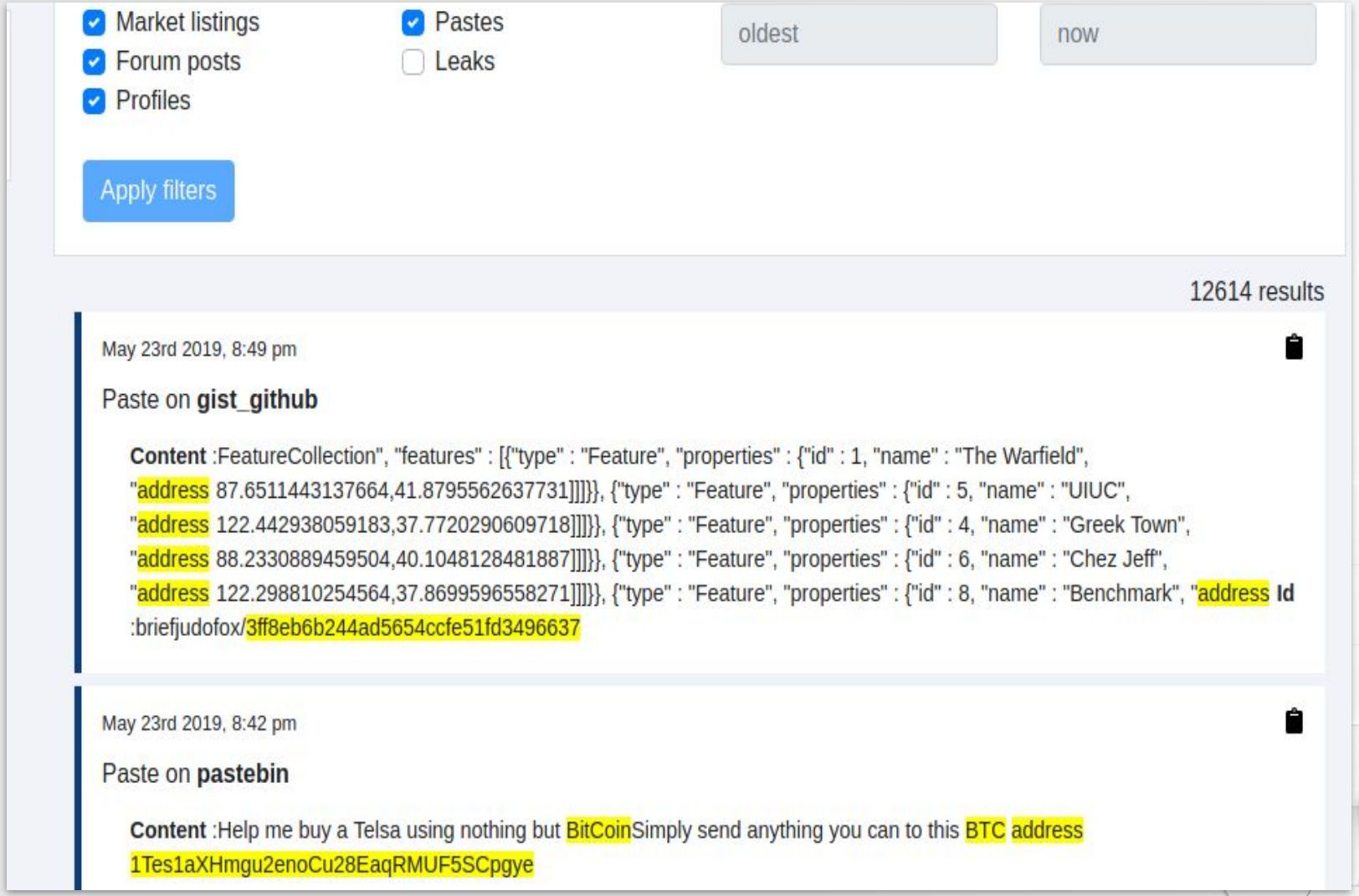
Sources d'identification

- Collaboration entre partenaires
- **Collecte de sources de données ouvertes**
- Analyse des transactions- montant et moment
- Analyse des branches ("fork") de cyrptomonnaies
- Analyse comportementale

Sources de données

Firework

Fireworks



FlareSystems

Démonstration

Analyse des transactions

Didn't you order back in November?

That's a long time to wait for a pack or a refund.

I'm not fully aware of the situation, but TO, hook this guy up! Post scarcity is a long time member here and he deserves whatever you have to offer.

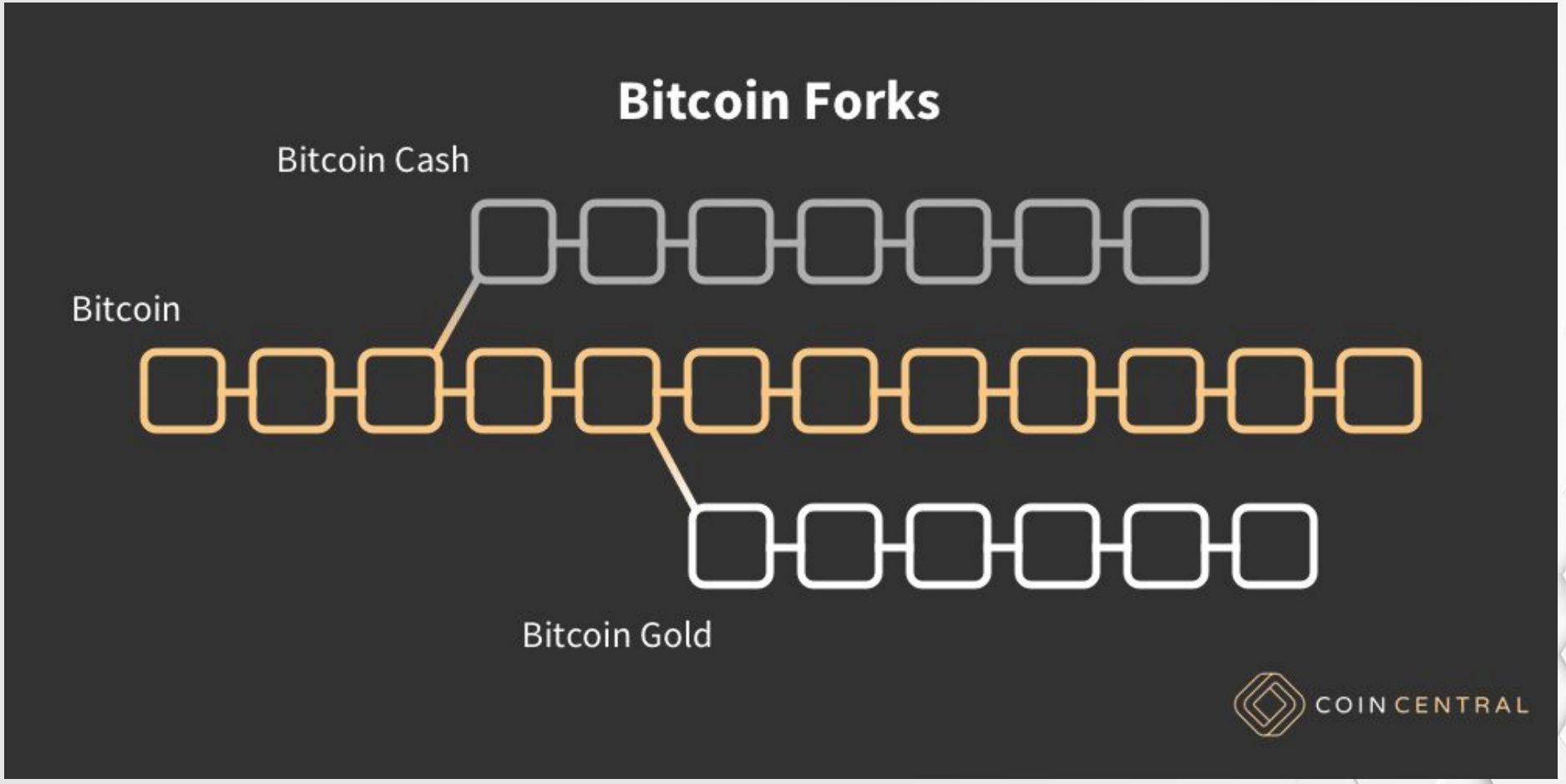
Post Scarcity,

Sending you the message we're awaiting a reply to on Dream which follows:

You sent 0.09565228 BTC = $611.74 when price per coin was $6,395.46, but that coin is now worth only $375.15.

It is and has always been our policy to refund the exact BITCOIN paid as the standard, not USD. So just want to be clear that you want this refund in that amount?

Branches alternatives



Limites de Bitcluster (open source)

- **Gestions des portefeuilles *multisig***
- Identification des acteurs
- Optimisation des requêtes et de la base de données
- Alertes sur des wallets ou des flux importants
- Surveillance des flux de bitcoin uniquement
- Outils de visualisation

Limites de Bitcluster (open source)

- Gestions des portefeuilles *multisig*
- **Identification des acteurs**
- Optimisation des requêtes et de la base de données
- Alertes sur des wallets ou des flux importants
- Surveillance des flux de bitcoin uniquement
- Outils de visualisation

Limites de Bitcluster (open source)

- Gestions des portefeuilles *multisig*
- Identification des acteurs
- **Optimisation des requêtes et de la base de données**
- Alertes sur des wallets ou des flux importants
- Surveillance des flux de bitcoin uniquement
- Outils de visualisation

Limites de Bitcluster (open source)

- Gestions des portefeuilles *multisig*
- Identification des acteurs
- Optimisation des requêtes et de la base de données
- **Alertes sur des wallets ou des flux importants**
- Surveillance des flux de bitcoin uniquement
- Outils de visualisation

Limites de Bitcluster (open source)

- Gestions des portefeuilles *multisig*
- Identification des acteurs
- Optimisation des requêtes et de la base de données
- Alertes sur des wallets ou des flux importants
- **Surveillance des flux de bitcoin uniquement**
- Outils de visualisation

Limites de Bitcluster (open source)

- Gestions des portefeuilles *multisig*
- Identification des acteurs
- Optimisation des requêtes et de la base de données
- Alertes sur des wallets ou des flux importants
- Surveillance des flux de bitcoin uniquement
- **Outils de visualisation**

Limites de Bitcluster (général)

- **Lightning network**
- Atomic swaps
- Profilage automatique des wallets

Limites de Bitcluster (général)

- Lightning network
- **Atomic swaps**
- Profilage automatique des wallets

Limites de Bitcluster (général)

- Lightning network
- Atomic swaps
- **Profilage automatique des wallets**

Conclusion

- **L'outil open-source est disponible tel quel et sans support**
- Certains développement commerciaux seront rétro-porté ("backport") dans la version open-source
- La version commerciale inclut les fonctionnalités suivantes
  - Gestion des adresses multi-signatures
  - Gestion de plusieurs crypto-monnaies (Etherium, BTCash, Bitcoin Gold, etc)
  - Gestion d'étiquettes ("labels") personnalisé
  - Visualisation et analyse de graphes.
  - Intégration avec notre solution de CTI ("auto-tagging")

Conclusion

- L'outil open-source est disponible tel quel et sans support
- **Certains développement commerciaux seront rétro-porté ("backport") dans la version open-source**
- La version commerciale inclut les fonctionnalités suivantes
  - Gestion des adresses multi-signatures
  - Gestion de plusieurs crypto-monnaies (Etherium, BTCash, Bitcoin Gold, etc)
  - Gestion d'étiquettes ("labels") personnalisé
  - Visualisation et analyse de graphes.
  - Intégration avec notre solution de CTI ("auto-tagging")

Conclusion

- L'outil open-source est disponible tel quel et sans support
- Certains développement commerciaux seront rétro-porté ("backport") dans la version open-source
- **La version commerciale inclut les fonctionnalités suivantes**
  - Gestion des adresses multi-signatures
  - Gestion de plusieurs crypto-monnaies (Etherium, BTCash, Bitcoin Gold, etc)
  - Gestion d'étiquettes ("labels") personnalisé
  - Visualisation et analyse de graphes.
  - Intégration avec notre solution de CTI ("auto-tagging")