D:\REST\MATHE\GFS\presentation\video\Danifilm.mp4

IN MATHEMATICS WE TRUST

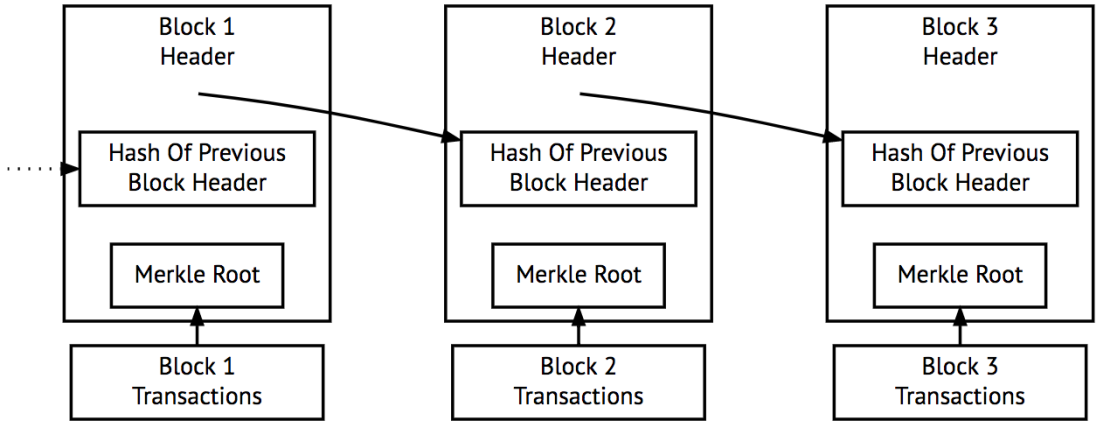
Talk is cheap show me the
math(code).
~ Linus Torvalds

Die Anwendung der
Kryptographie in der
Blockchain
am Beispiel von Bitcoin

1) Blockchain & Bitcoin
2) Übersicht Kryptographie
3) Kryptographische Methoden in der Bitcoin Blockchain
4) Zusammenfassung

Was ist eine Blockchain?

- Dezentrale Datenbankstruktur
- Digitales Register → Unveränderlichkeit & Transparent
- Kette von Blöcken



Simplified Bitcoin Block Chain

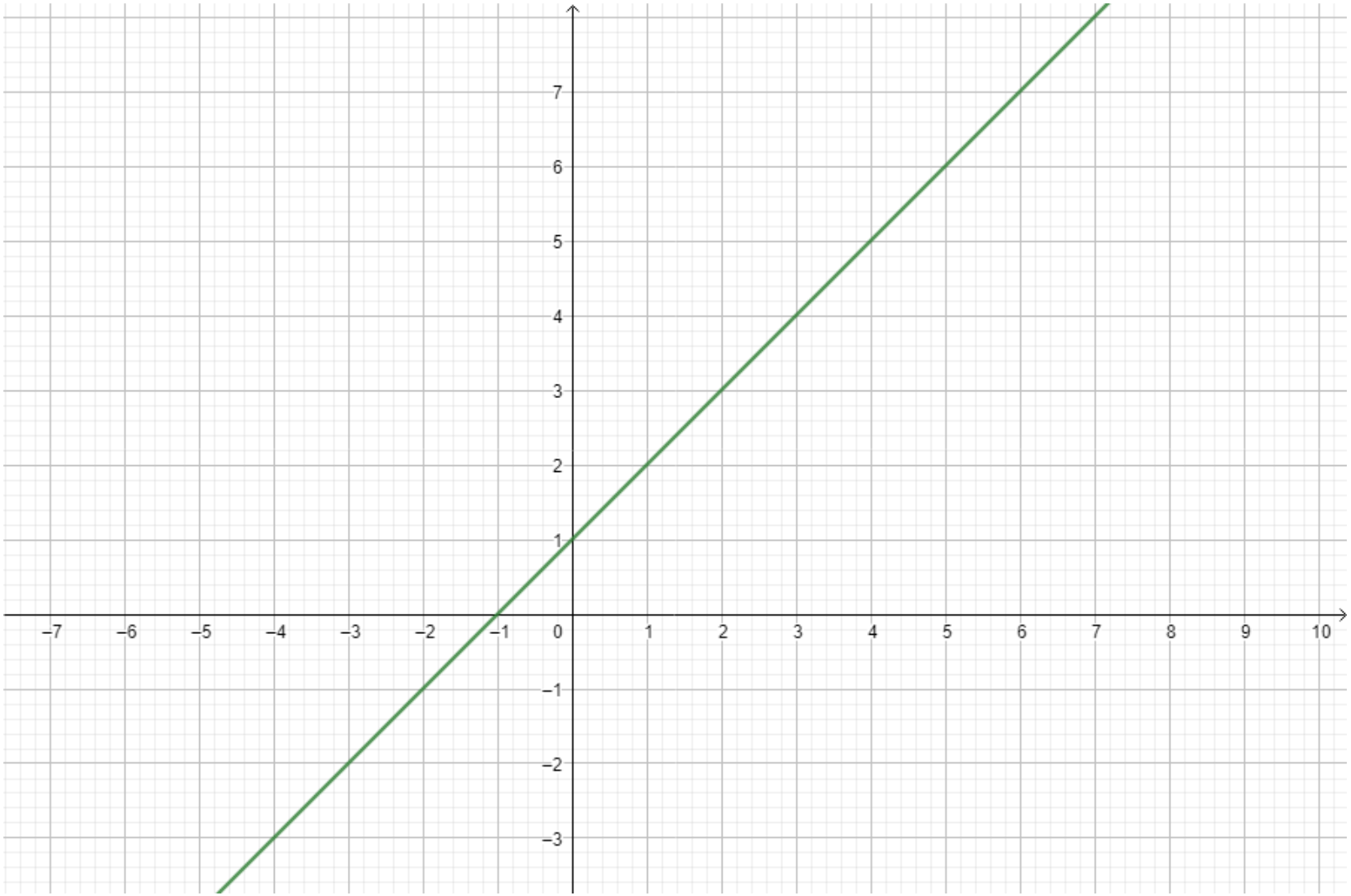
Was ist Bitcoin?

- Anwendung der Blockchain
- Digitale Währung/Anlage
- Basiert auf Mathematik

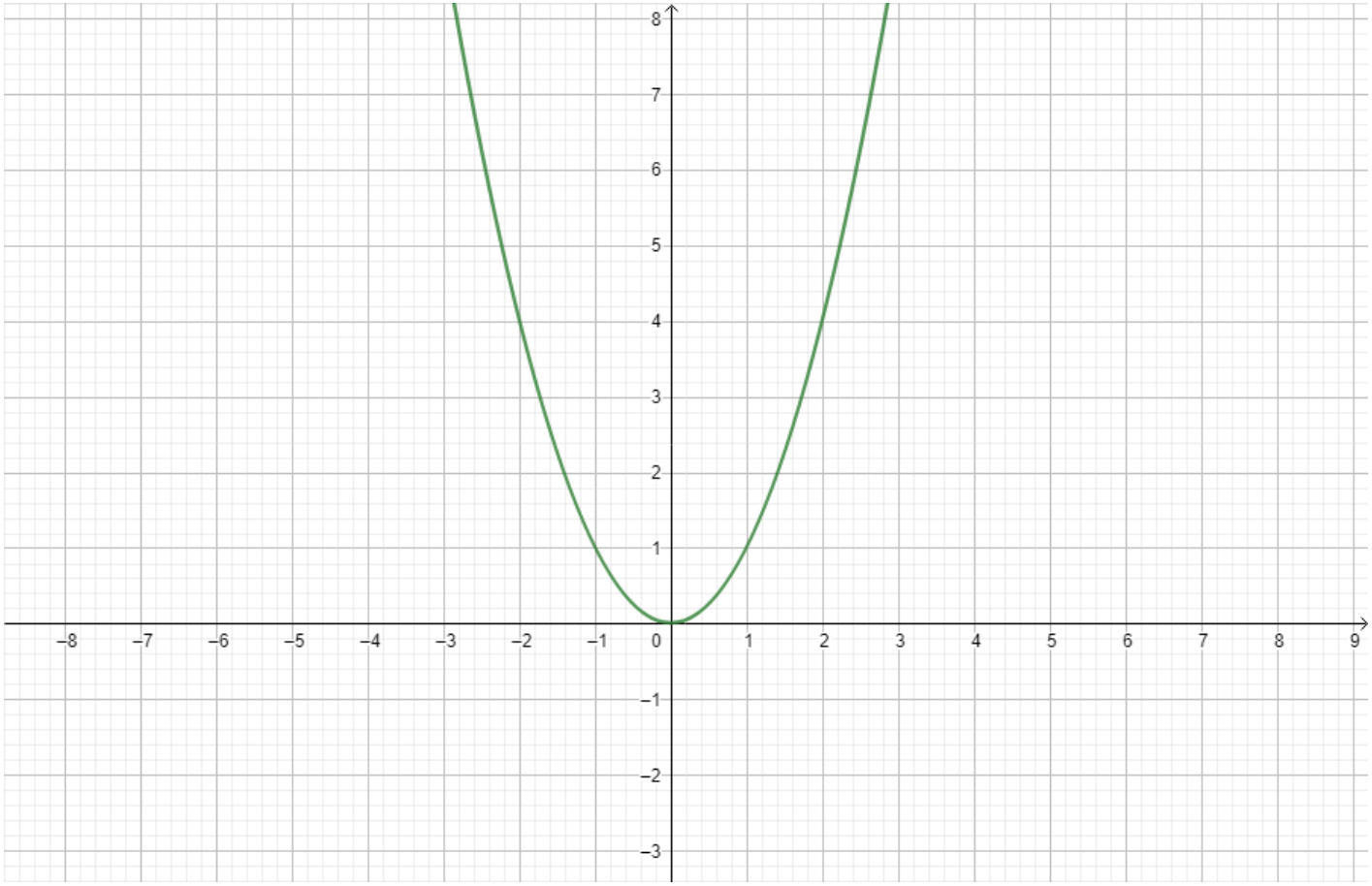
Übersicht Kryptographie

- **Symmetrische Verfahren**
  - Ein Schlüssel
    - Chiffretext
- **Asymmetrische Verfahren**
  - Öffentliche & Private Schlüssel
    - RSA
    - Elliptic Curve Kryptographie

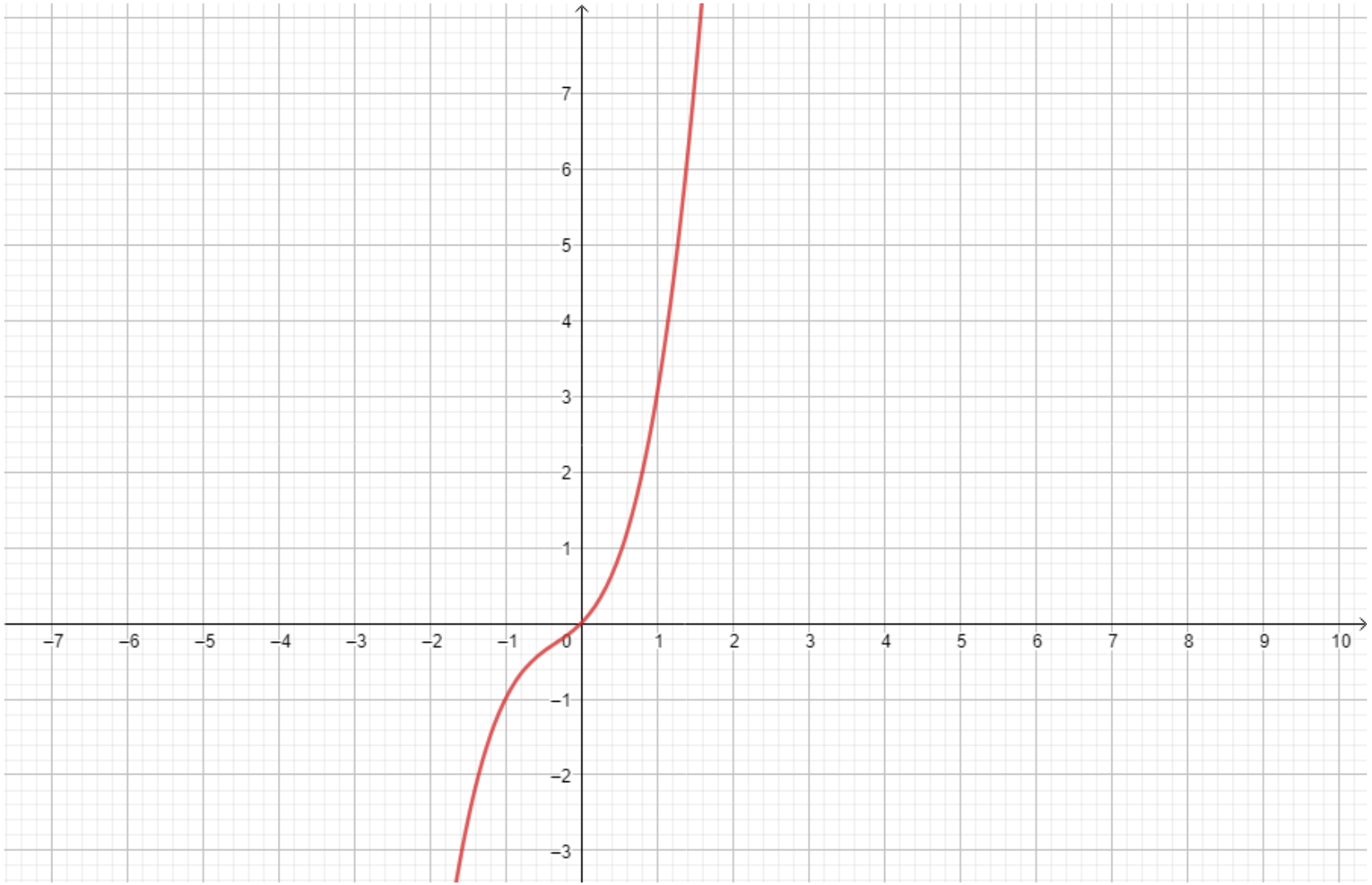
Linear (y = mx + b)



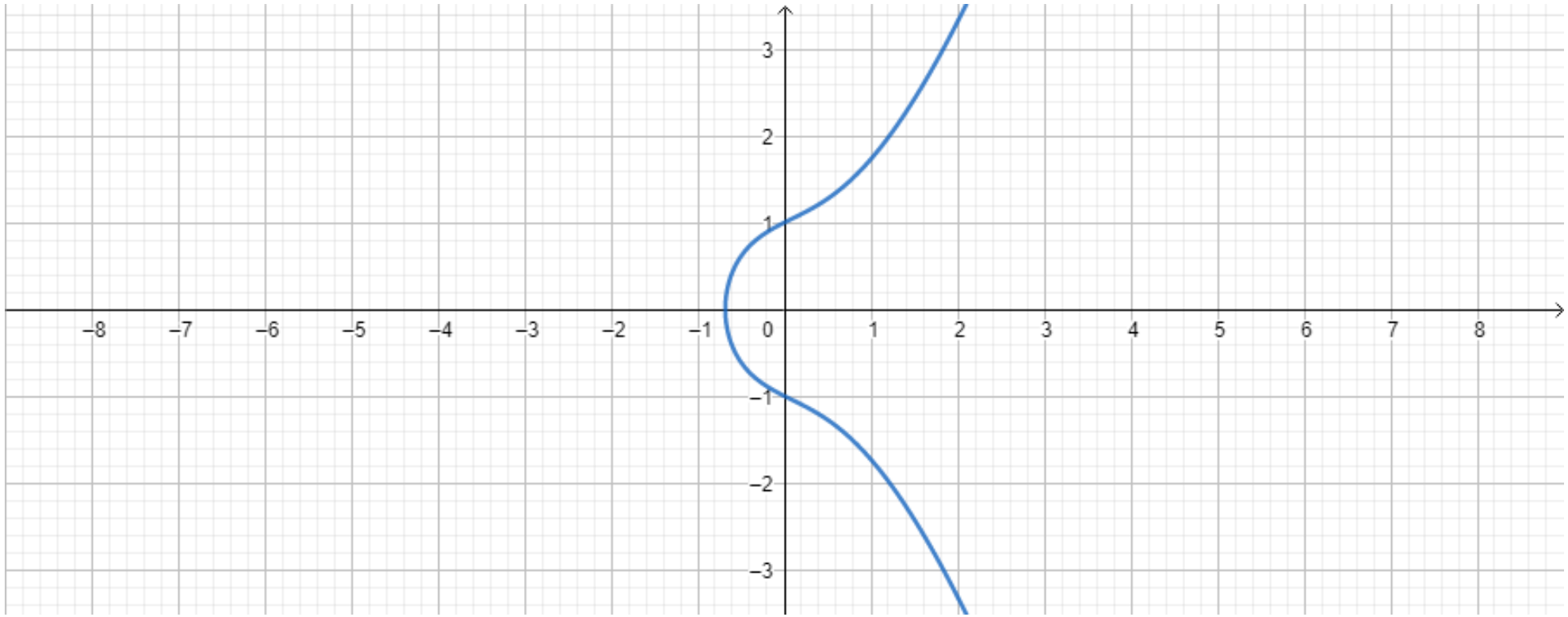
Quadratisch (y = x^2 + bx + c)



Kubisch (y = ax^3 + bx^2 + cx + d)



Elliptic (y^2 = ax^3 + bx + c)

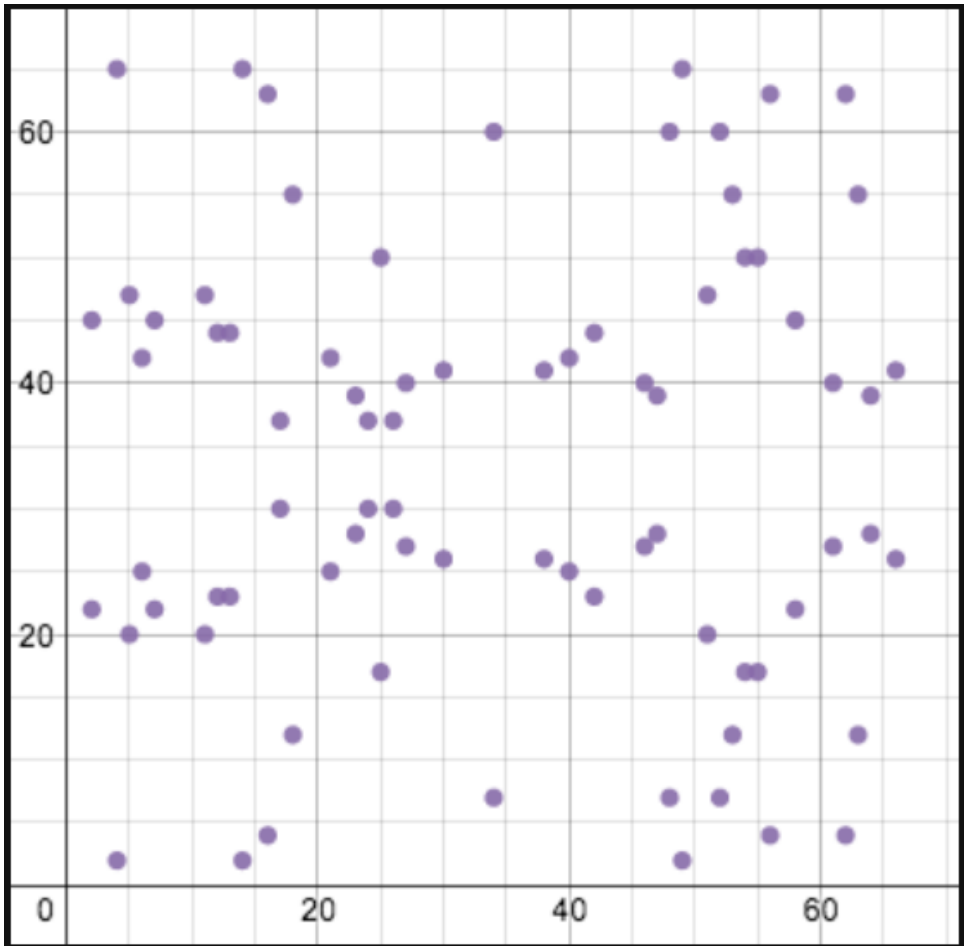


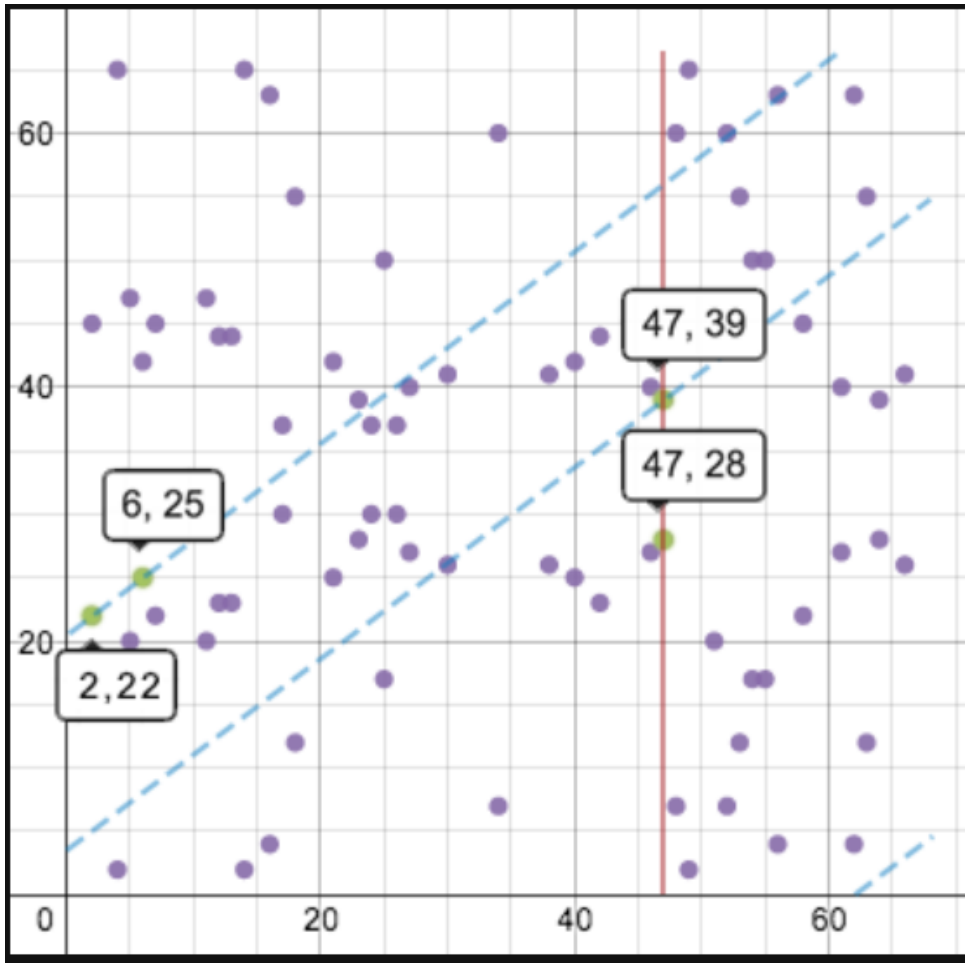
Eigenschaften der Elliptic Curve Kryptographie

- **Endlichen Primkörpern & modulo**
  - Y^2 = x^3 + bx + c mod p
- **Wenn eine Gerade die Kurve in zwei Schnittpunkten schneidet, gibt es auch einen dritten Schnittpunkt(Ausnahmen)**
- **Punkt Addition & Multiplikation**
  - G = Generator Punkt

Anwendung in Bitcoin → Überweisung

Elliptische Kurve in endlichem Feld mod 64





Danke für eure Aufmerksamkeit

- Ausarbeitung: https://github.com/daniel-vera-g/KryptographieGFS
- Code für Demo:
  - https://github.com/anders94/public-private-key-demo
  - https://github.com/andreacorbellini/ecc
- Weitere Projekte: https://github.com/daniel-vera-g/

BestWikiPageOnThePlanet

Quellen

- Demo:
  - https://anders.com/blockchain/public-private-keys/
  - https://github.com/andreacorbellini/ecc
- http://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/
- http://procbits.com/2013/08/27/generating-a-bitcoin-address-with-javascript
- https://www.btc-echo.de/tutorial/was-sind-bitcoins/
- https://www.btc-echo.de/tutorial/was-ist-die-blockchain/
- http://www.searchsecurity.de/antwort/Worin-unterscheiden-sich-symmetrische-und-asymmetrische-Verschluesselung
- https://hackernoon.com/bitcoin-ethereum-blockchain-tokens-icos-why-should-anyone-care-890b868cec06
- https://www.youtube.com/watch?v=e6voIwB-An4&index=14&list=PLkyGSjskdfq8-WPORX-ZM_t_P8cV-kR6z&t=845s
- https://www.coindesk.com/math-behind-bitcoin/