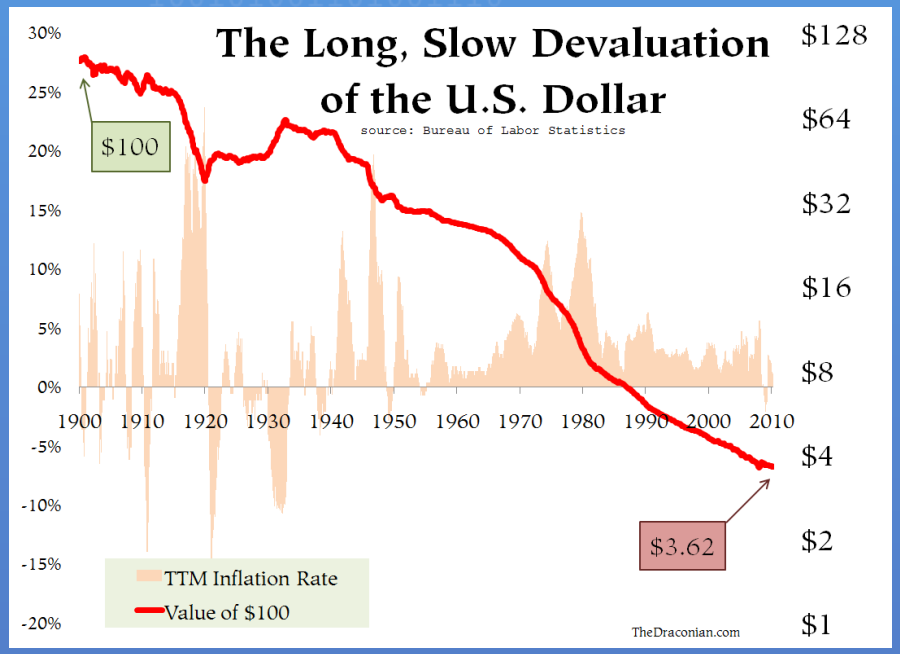
Peer-to-Peer Digital Currency

ساختار ارائه

- واحد پول رایج
- پول دیجیتال
- آنارشیسم، فری سافتویر و پیدایش P۲P Currency
  - Ripple
  - Bitcoin Satoshi Nakamoto
- از دید کاربر
- نحوه کارکرد
- تکنولوژی های مرتبط
- ساختار

واحد های مدرن پول



- کنترل مرکزی
- ارزش واقعی و پشتوانه
- امکان چاپ نا محدود
- Tinkerbell Effect
- بانک ها

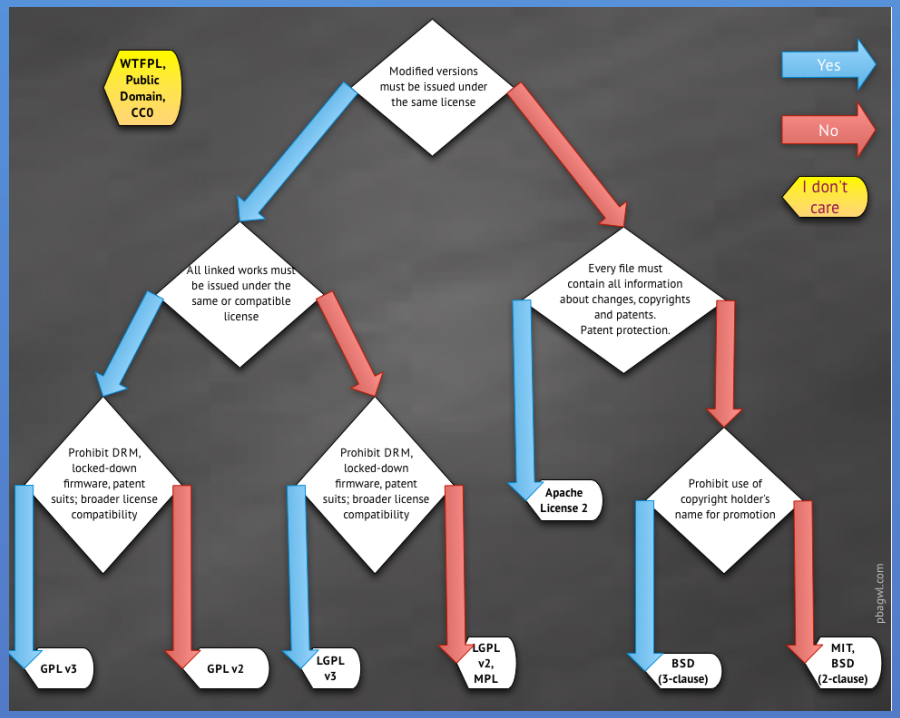
پول دیجیتال

- کنترل مرکزی
- فشار دولتی
- نمونه ها
  - PayPal
  - E-gold
  - E-Bullion
  - Pecunix

Anarchism

- Mutualism
- Collectivist anarchism
- Anarchist communism
- Anarcho-capitalism
- Economic Democracy

Free Software



- آزادی در استفاده
- آزادی در تغییر و بررسی
- آزادی در نشر مجدد
- آزادی در تغییر و نشر
- آزادی در استفاده در دیگر لایسنس ها
- محدودیت های قید کپی رایت

نرم افزار متن باز و آنارشیسم

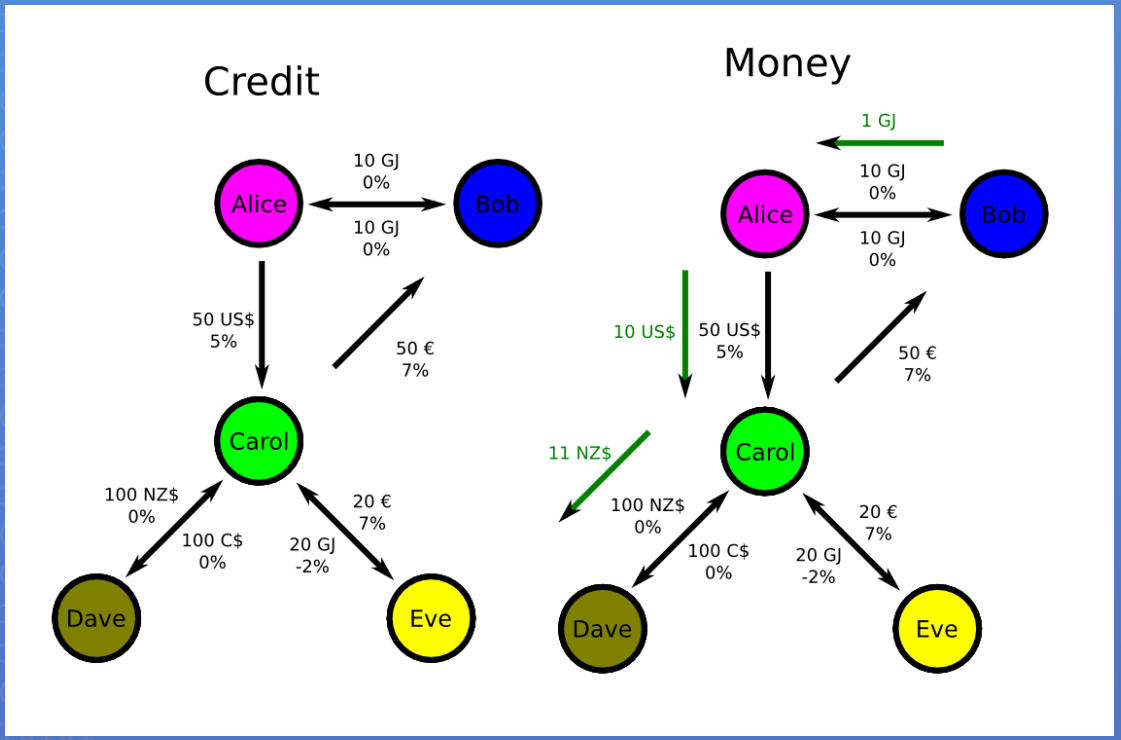
- ناخوداگاه
- باز
- بدون هدایت انفرادی
- غیر انحصاری

پیدایش P۲P Currency

- Crypto–anarchism
  - آزادی
  - امنیت اطلاعات شخصی
- نمونه Peer–to–Peer Currency
  - Ripple
  - Bitcoin

Ripple

- بر پایه اطمینان بین کاربران
- امکان تایین سقف برای دوستان

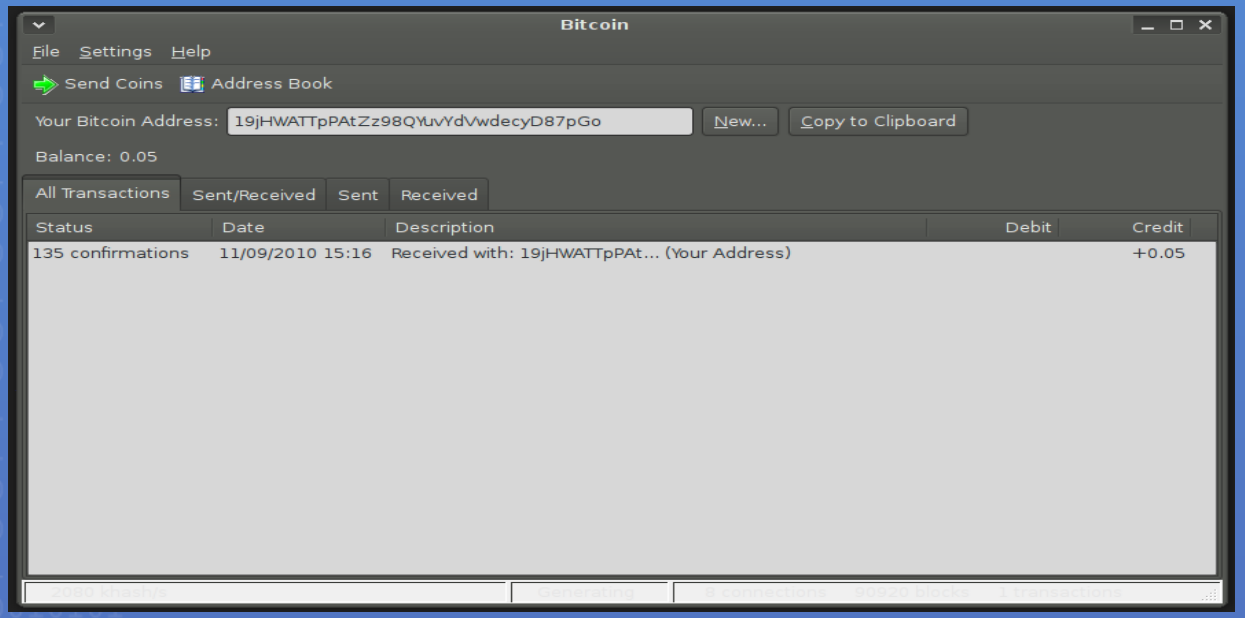


Bitcoin

- واحد پولی دیجیتال بین کاربری
- مزایا
  - انتقال مبالغ بدون هزینه و بدون اتلاف زمان
  - تماما بین کاربری
  - امنیت بالا
  - بدون کنترل مرکزی
  - بدون تورم
  - تغییر قوانین توسط کاربران

از دید کاربر Bitcoin

- نصب کلاینت
- ساخت خودکار آدرس توسط کلاینت
- شروع به دریافت و یا ارسال مبالغ!



نحوه کارکرد bitcoin

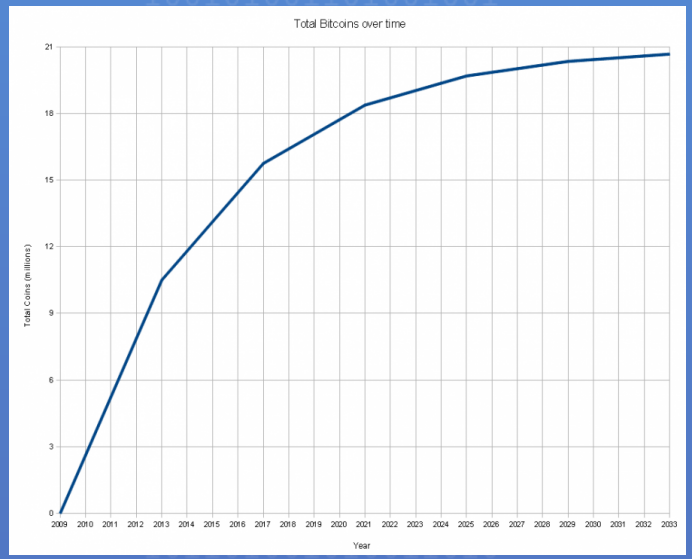
- انتقال وجه قابل بازگشت نیست
- امکان پیدا کردن صاحب وجه ها وجود ندارد
- امکان پرداخت بیش از موجودی وجود ندارد
- نمیتوان مبلغ را به بیش از یک نفر ارسال نمود
- تا زمانی که نیمی از کاربران درست باشند امکان تقلب وجود ندارد
- نرخ رشد نقدینگی محدود و در ۲۰۳۳ قطع میشود
- هزینه انتقال صفر بوده مگر به درخواست کاربر

نحوه کارکرد bitcoin

- کاربر در هر زمانی میتواند به شبکه وصل شده شروع به نقل و انتقال کند
- هیچ کس به غیر از دارنده حساب نمیتواند وجه را منتقل کند
- هر کاربر میتواند به تعداد بیشمار آدرس داشته باشد
- به صورت دموکراتیک (۵۰% قدرت پردازش) کاربران میتوانند قوانین را تغییر دهند

منبع پول در گردش bitcoin

- تا سال ۲۰۳۳ به صورت کاهنده ای bitcoin miners برای هر بلاک ایجادی bitcoin دریافت خواهند کرد.
- Miners گروه کاربرانی هستند که با قدرت پردازش خود اقدام به انجام محاسبات مورد نیاز شبکه را انجام میدهند
- بعد از ۲۰۳۳، Miners فقط اقدام به جمع اوری مبالغ بخشیده شده از طرف کاربران برای تسریع انتقالات می کنند

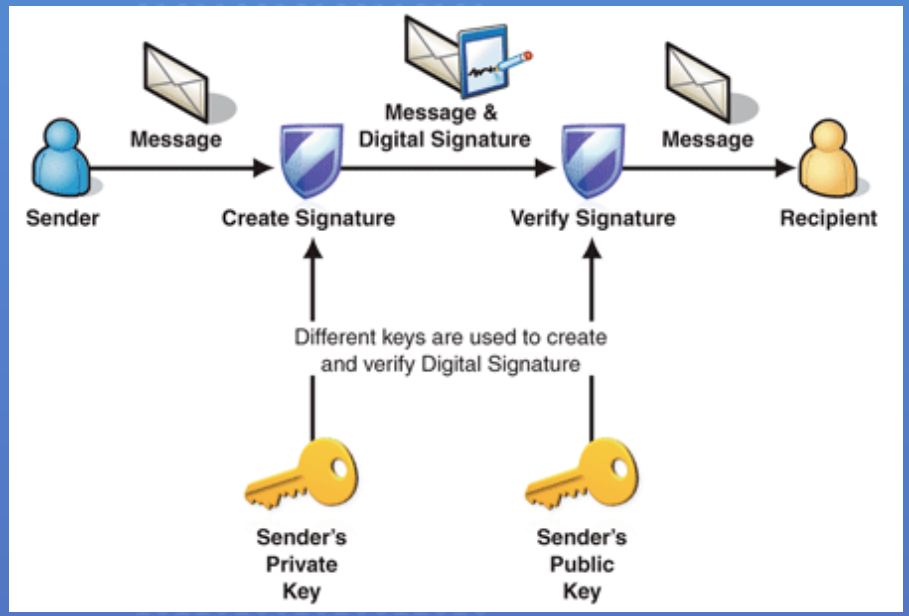


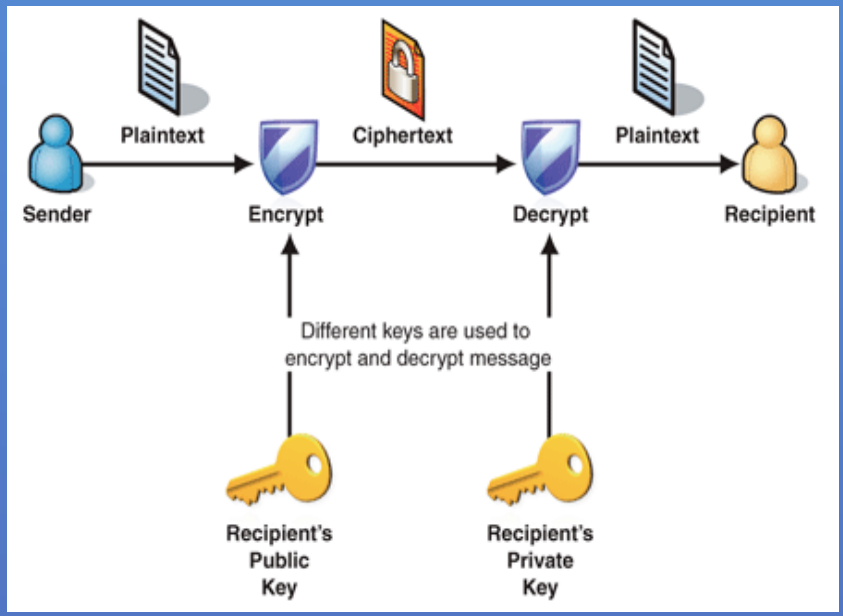
ساختار Bitcoin

- قبل از شروع ...
  - Public-Key Encryption
  - Cryptographic Hash Function
  - Hashcash
  - Bmoney
  - Timestamp Chaining

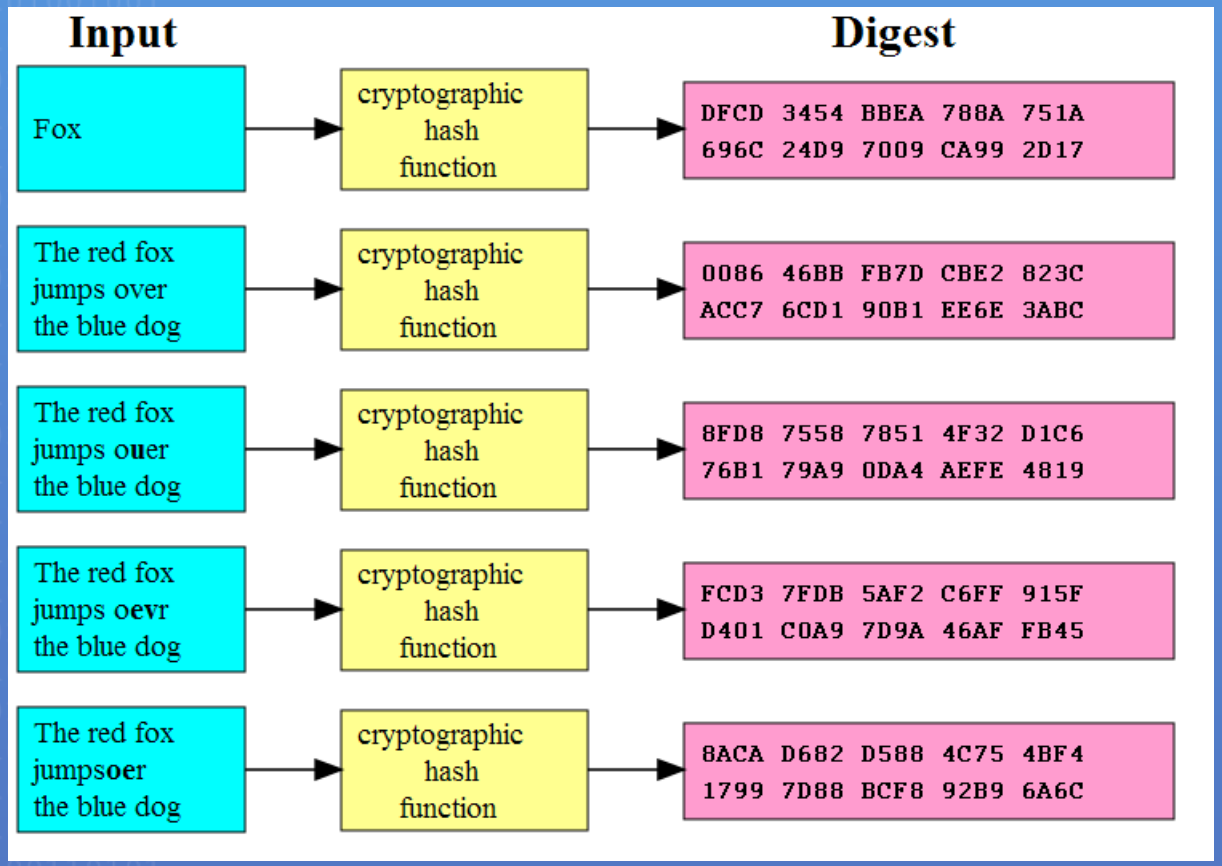
Public-Key Encryption

- Public Key: Validate Sign., Encrypt Data
- Private Key: Sign Data, Decrypt Data





Cryptographic Hash Function



Hashcash

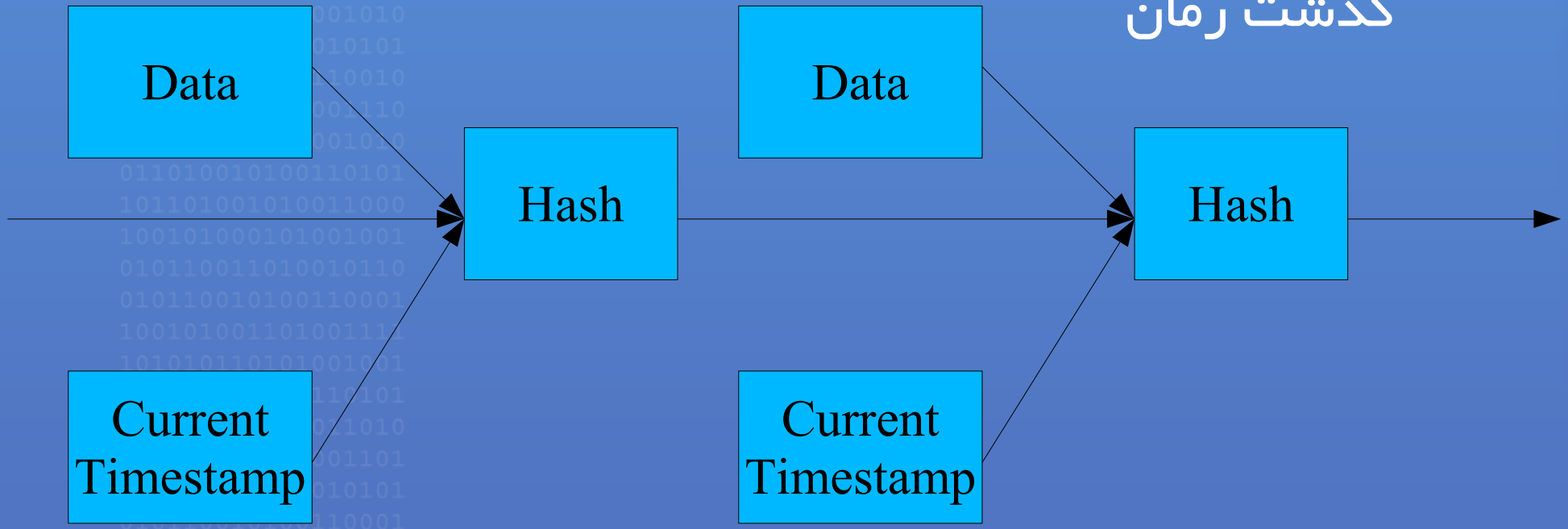
- طراحی در ۱۹۹۷ برای محدود کردن DoS و Spam
- بار پردازشی قابل تنظیم بر روی کلاینت ها
- تایید ساده از طرف سرور

bmoney

- متاثر از Crypto-anarchism
- طرح تکنیک های لازم برای ممکن کردن واحد پولی p2p
- تولید پول با یافت جواب برای سوالات حل نشده

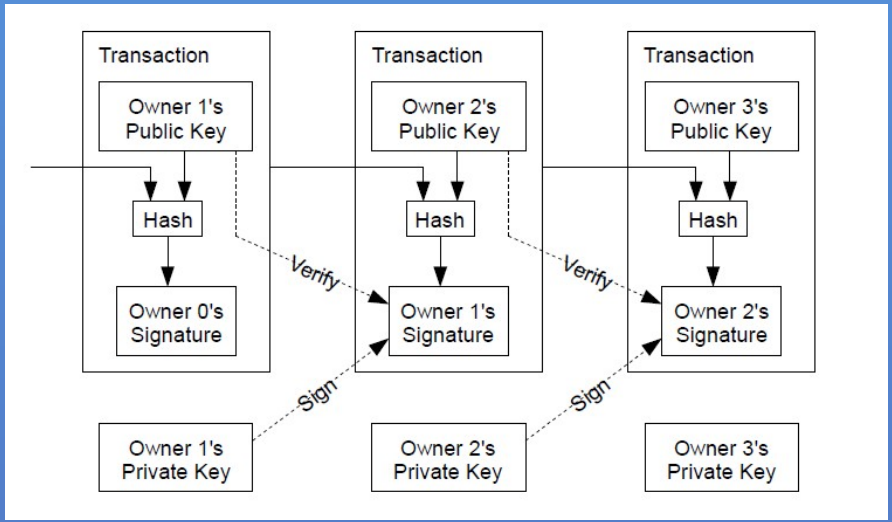
Timestamp Chaining

- تضمین زمان انجام عملیات ها
- حفظ ترتیب انجام
- نزدیک به غیر ممکن نمودن تغییر در عملیات های انجام شده با گذشت زمان



ساختار Bitcoin | انتقال وجه

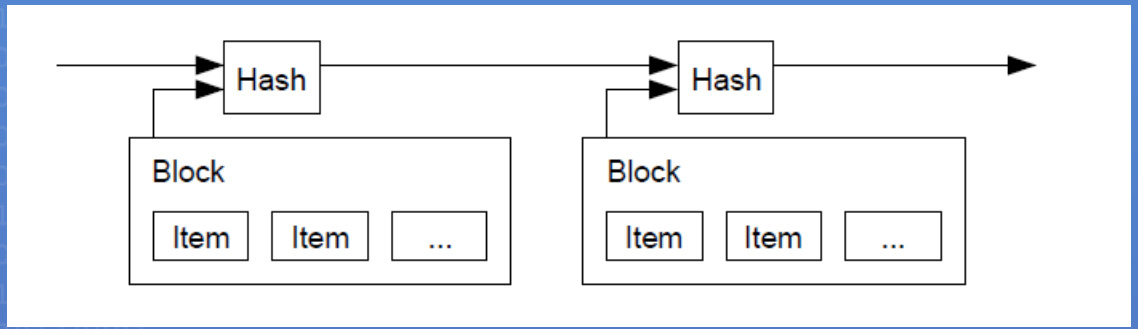
- صاحب مبلغ با امضا (sign) هش انتقال قبلی و پابلیک کی مقصد (صاحب بعدی مبلغ) آن ها را به ته سکه اضافه مینماید



- صاحب بعدی با کنترل امضا و ... از صحت انتقال با خبر میشود
- عملیات پابلیک میشود
- تایید عملیات و امضا توسط سایرین

ساختار Bitcoin | جلوگیری از تقلب

- کنترل امضا توسط مقصد و کاربران ناظر
- کنترل timestamp chain برای اطمینان از تکراری نبودن انتقال و صحت

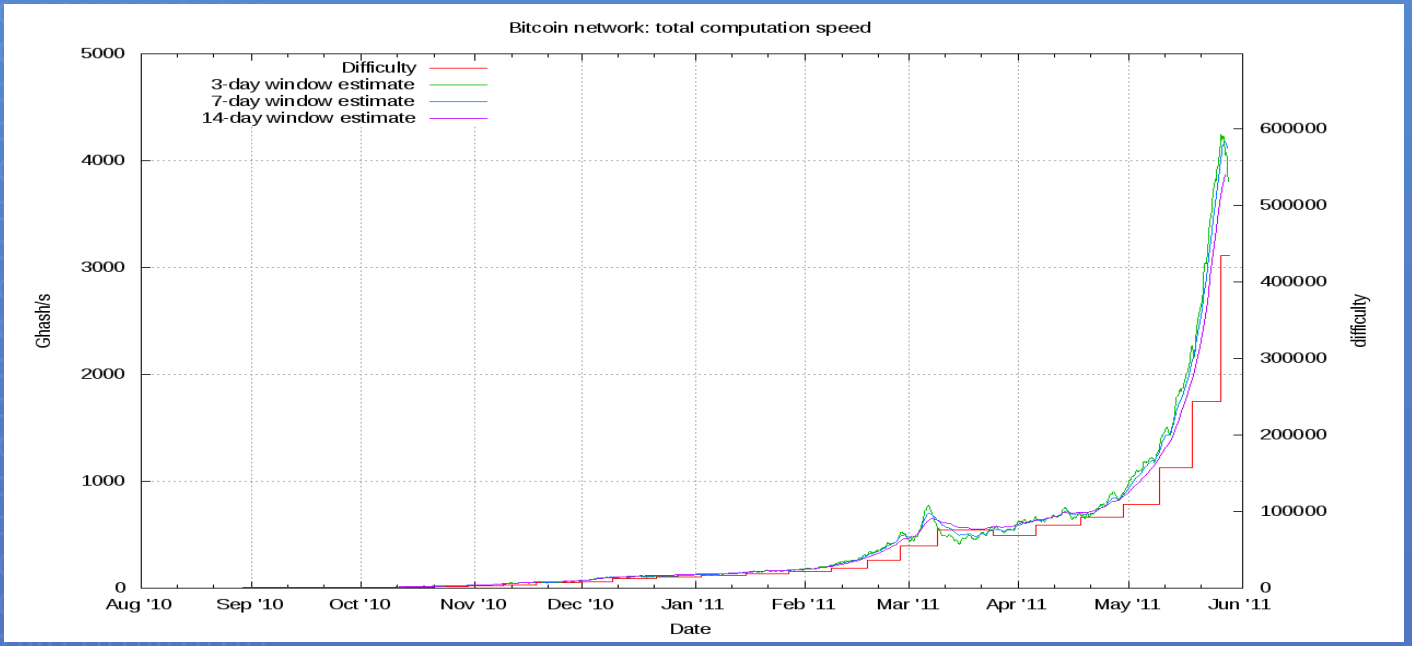


ساختار Bitcoin | ایجاد بلاک

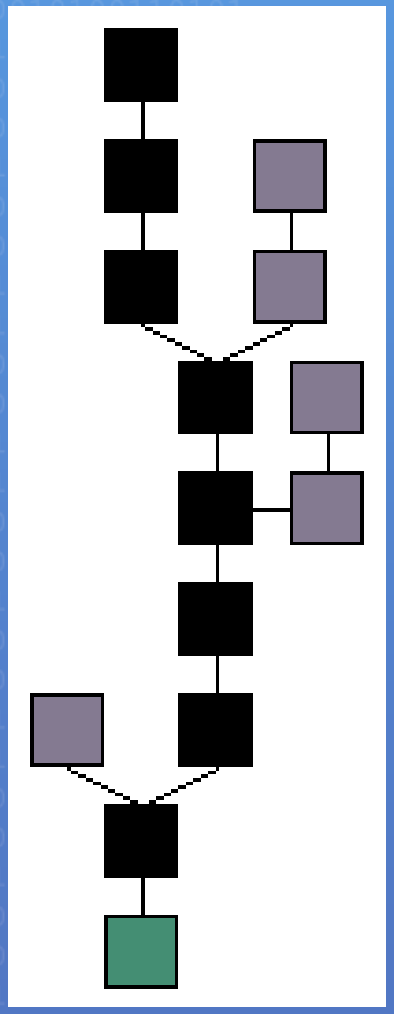
- حدودا هر ۱۰ دقیقه یک بار یک بلاک ایجاد میشود
- بلاک توسط miner ایجاد میشود
- بلاک شامل تمام نقل انتقال ها از ایجاد بلاک قبلی می باشد
- ترتیب بلاک ها با روش timestamp chaining تضمین میشود
- محاسبه بلاک با استفاده از Hashcash بسته به تعداد قدرت پردازش ماینرز ها کم و زیاد می شود.

ساختار Bitcoin | محاسبه بلاک

- بعد از ایجاد بلاک miner موفق آن را اعلام نموده به تایید ما بقی میرسد.
- بلاک باعث تسریع کنترل صحت عملیات ها می شود.

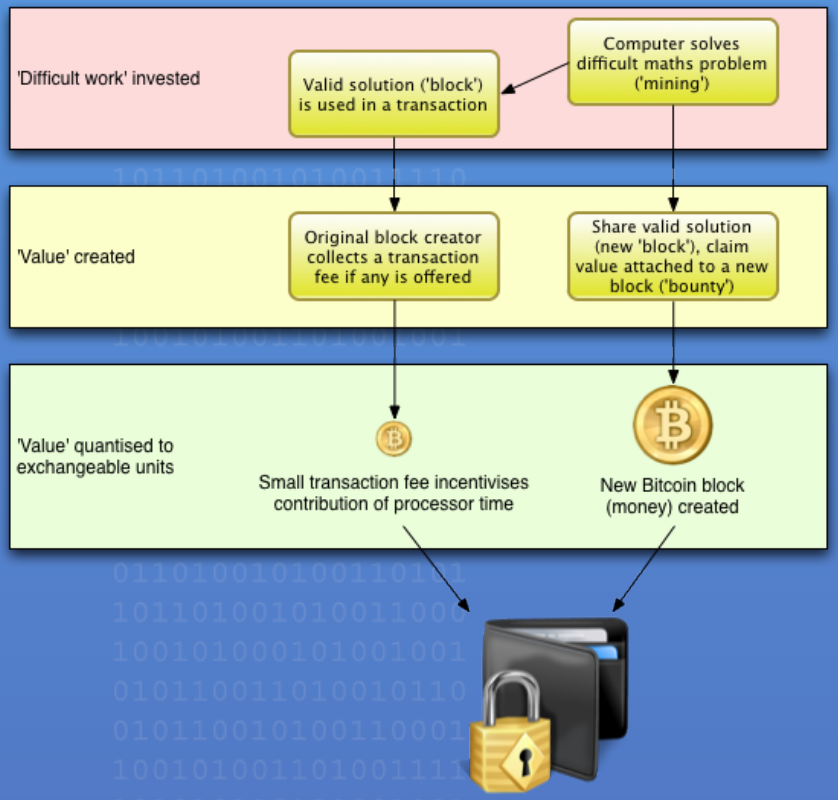


ساختار Bitcoin | بلاک



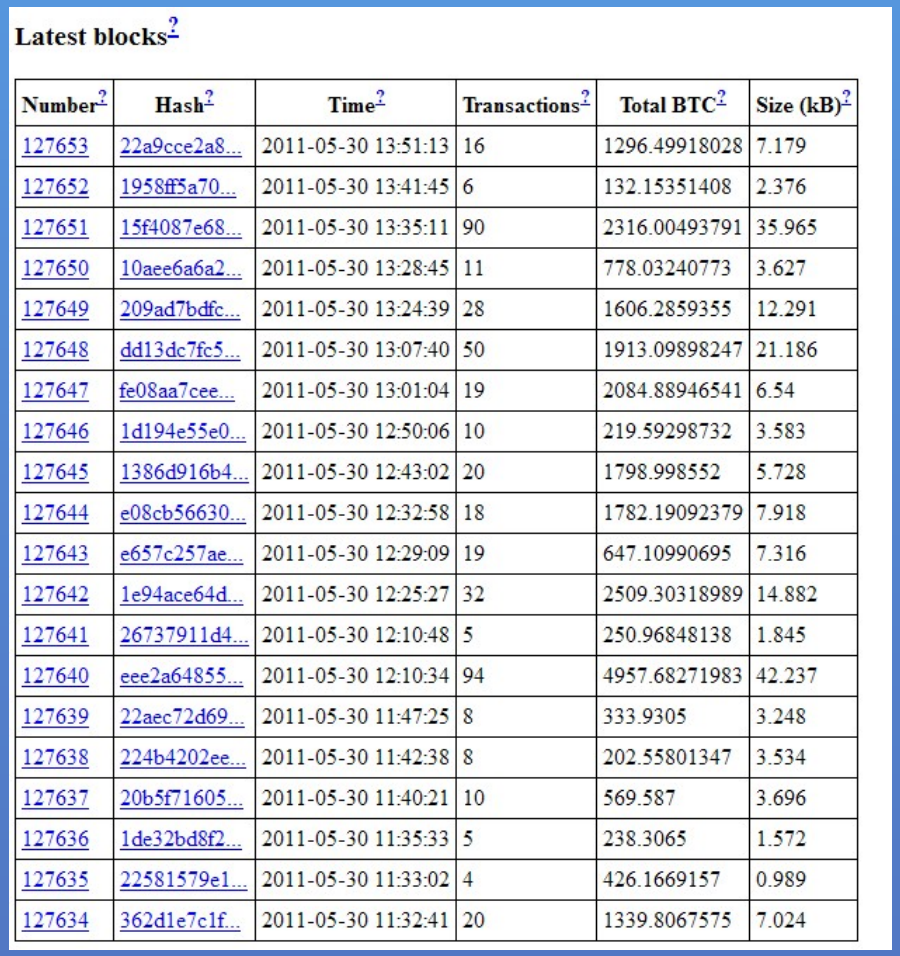
- در صورتی که همزمان بیش از یک بلاک ایجاد شود در زمان ایجاد بلاک بعدی بلندترین رشته بلاک قطعی شده مابقی انتقالات برای قرار گیری در بلاک بعدی آزاد میشوند

ساختار Bitcoin | ماینرز



- با قرار دادن مبالغ تشویقی قدرت پردازش تقویت شده امکان تقلب به حداقل میرسد

ساختار Bitcoin | زنجیره بلاک ها



Latest blocks[?]

Number[?]	Hash[?]	Time[?]	Transactions[?]	Total BTC[?]	Size (kB)[?]
127653	22a9cce2a8...	2011-05-30 13:51:13	16	1296.49918028	7.179
127652	1958ff5a70...	2011-05-30 13:41:45	6	132.15351408	2.376
127651	15f4087e68...	2011-05-30 13:35:11	90	2316.00493791	35.965
127650	10aee6a6a2...	2011-05-30 13:28:45	11	778.03240773	3.627
127649	209ad7bdfc...	2011-05-30 13:24:39	28	1606.2859355	12.291
127648	dd13dc7fc5...	2011-05-30 13:07:40	50	1913.09898247	21.186
127647	fe08aa7cee...	2011-05-30 13:01:04	19	2084.88946541	6.54
127646	1d194e55e0...	2011-05-30 12:50:06	10	219.59298732	3.583
127645	1386d916b4...	2011-05-30 12:43:02	20	1798.998552	5.728
127644	e08cb56630...	2011-05-30 12:32:58	18	1782.19092379	7.918
127643	e657c257ae...	2011-05-30 12:29:09	19	647.10990695	7.316
127642	1e94ace64d...	2011-05-30 12:25:27	32	2509.30318989	14.882
127641	26737911d4...	2011-05-30 12:10:48	5	250.96848138	1.845
127640	eee2a64855...	2011-05-30 12:10:34	94	4957.68271983	42.237
127639	22aec72d69...	2011-05-30 11:47:25	8	333.9305	3.248
127638	224b4202ee...	2011-05-30 11:42:38	8	202.55801347	3.534
127637	20b5f71605...	2011-05-30 11:40:21	10	569.587	3.696
127636	1de32bd8f2...	2011-05-30 11:35:33	5	238.3065	1.572
127635	22581579e1...	2011-05-30 11:33:02	4	426.1669157	0.989
127634	362d1e7c1f...	2011-05-30 11:32:41	20	1339.8067575	7.024

- بلاک های زنجیر شده از طریق روش timestamp chaining
- شامل زمان تعداد انتقالات و جمع مبالغ انتقال

ساختار Bitcoin | ساختار بلاک

Block 127438

Short link: http://blockexplorer.com/b/127438

Hash: 00000000000002107285c86c21a0a0bde4d34a7eda1a9c29af1271adf6ca0e65e

Previous block: 0000000000000f14c3407c7b6ea6093340aafe20211a35f0ac7dca60d1c7962d

Time: 2011-05-29 07:46:30

Difficulty: 434 877.045527 ("Bits": 1a269421)

Transactions: 13

Total BTC: 2081.06233119

Size: 5.259 kilobytes

Merkle root: fe1cdfce193d17e26b87ef5bfab5bca3c96c4d7479a705fc598f4555fc043dcd

Nonce: 4042881319

Raw block

Transactions

Transaction	Fee	Size (kB)	From (amount)	To (amount)
22021173b0...	0	0.135	Generation: 50 + 0.03 total fees	1NBWTmzPoXnELAqXHqo2S8MV2SDPNY44Cj: 50.03
039503fcfe...	0	0.258	19ei3YAubAWrrjqW3BPi7TT2gkYf65mpwz: 352.30655521	1JeE94sxnwbaj3C9ADLepMMPuGi1aBWcZh: 352.27655521 16pMFuWbLdHgHrBaErbqFPeFjsrC86C6BT: 0.03
bf9101ef42...	0	0.258	1G8CZXx1XCz9JndkSob3oj3c3iJdJ66DHw: 282.7935	13u5XWAdMfqgSCpfwDVT6bte3Vrotv1nw7: 282.4535 19fXnE7DeKfqJ1HNPtgkML3uCUMt99TTcB: 0.34

ساختار Bitcoin | ساختار انتقال

Transaction

Short link: http://blockexplorer.com/t/8seXRgjBA

Hash[?]: 039503fcfe03cdfb53f882ff4a8eabbdbddbb718b1e5919f2a0703d5d67bcb49
Appeared in block 127438 (2011-05-29 07:46:30)
Number of inputs[?]: 1 (Jump to inputs)
Total BTC in[?]: 352.30655521
Number of outputs: 2 (Jump to outputs)
Total BTC out[?]: 352.30655521
Size[?]: 258 bytes
Fee[?]: 0
Raw transaction[?]

Inputs[?]

Previous output (index)[?]	Amount[?]	From address[?]	Type[?]	ScriptSig[?]
818d5ce8d855...:0	352.30655521	19ei3YAubAWrrjqW3BPi7TT2gkYf65mpwz	Address	3045022008324f4eb960555b6e2c459322e7b9f 043f6a65030c71429e7663ebf66dac718ae9d08(

Outputs[?]

Index[?]	Redeemed at input[?]	Amount[?]	To address[?]	Type[?]	ScriptPubKey[?]
0	Not yet redeemed	352.27655521	1JeE94sxnwbaj3C9ADLepMMPuGi1aBWcZh	Address	OP_DUP OP_HASH160 c1847f32928508c44e175150fbf151cc6a9a5c4b OP_EQUALVERIFY OP_CHECKSIG
1	Not yet redeemed	0.03	16pMFuWbLdHgHrBaErbqFPeFjsrC86C6BT	Address	OP_DUP OP_HASH160 3fcd16bbf7660acb567c0d91eddaf9e744de95c5 OP_EQUALVERIFY OP_CHECKSIG

منابع

- http://www.bitcoin.org/bitcoin.pdf
- http://weidai.com/bmoney.txt
- http://www.hashcash.org/hashcash.pdf
- http://en.wikipedia.org/wiki/Bitcoin
- http://geekosaur.com/2011/05/bitcoin-the-cryptographic-currency-that-wont-take-off-but-really-really-should/
- http://www.dyndy.net/2011/03/action-in-london-revolutionary-credit-cards/
- http://lwn.net/Articles/414452/
- http://www.promotionalcodes.org.uk/26970/what-is-bitcoin/
- http://bitcoin.sipa.be/
- http://en.wikipedia.org/wiki/Fiat_money
- http://www.law.mq.edu.au/html/MqLJ/volume4/vol4_stewartc.pdf
- http://en.wikipedia.org/wiki/Iranian_rial
- http://thedraconian.com/
- http://en.wikipedia.org/wiki/Boiling_frog
- https://ripplexchange.com/
- http://guides.brucejmack.biz/SOA-Patterns/WSSP/13.1PublicKeyEncryptDigSigDoc.htm
- http://en.wikipedia.org/wiki/File:Cryptographic_Hash_Function.svg