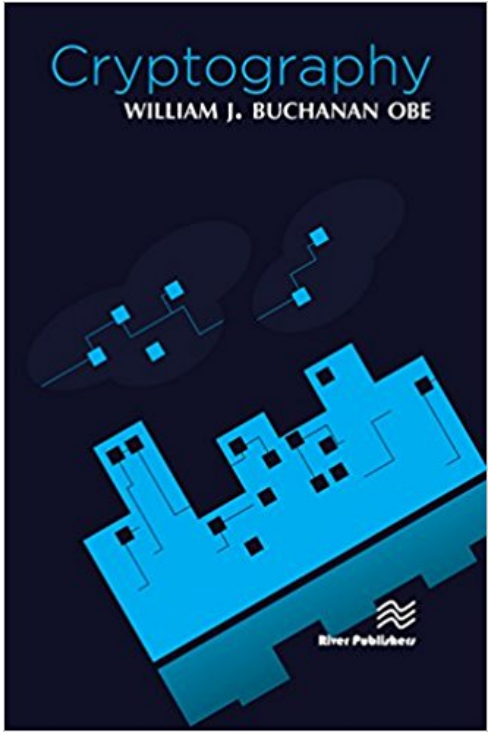
Chapter 10: Blockchain and Cryptocurrencies

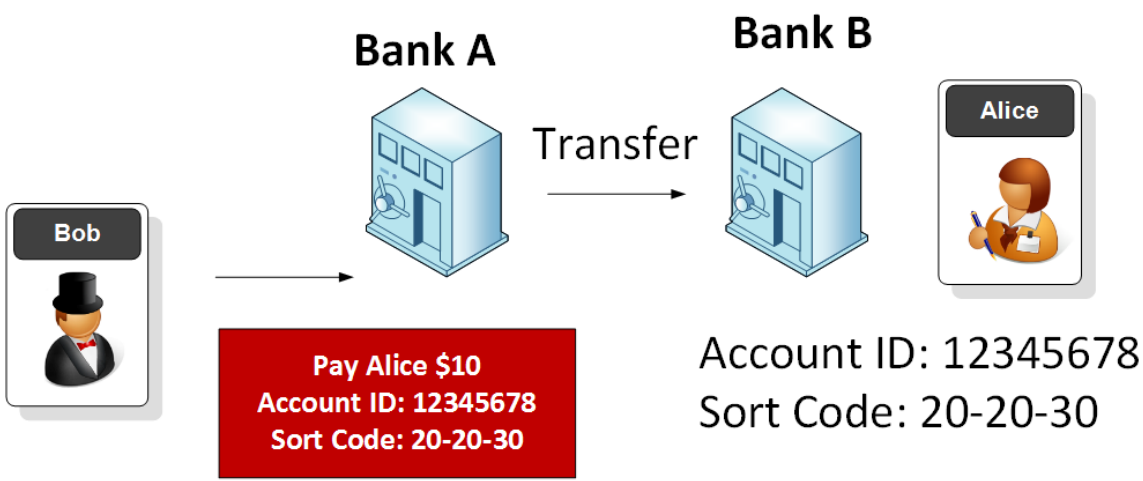


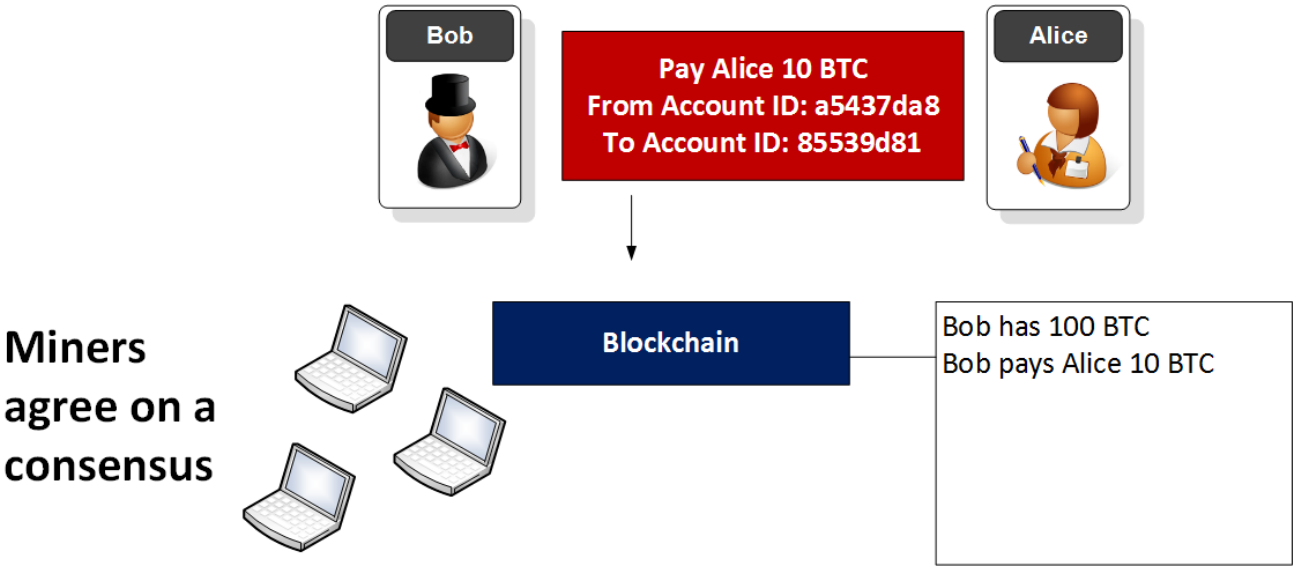
Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts

Prof Bill Buchanan OBE

http://asecuritysite.com/crypto10
http://asecuritysite.com/encryption

Payments


Bank A
Bank B
Transfer
Alice
Bob
Pay Alice $10
Account ID: 12345678
Sort Code: 20-20-30
Account ID: 12345678
Sort Code: 20-20-30


Bob
Pay Alice 10 BTC
From Account ID: a5437da8
To Account ID: 85539d81
Alice
Miners
agree on a
consensus
Blockchain
Bob has 100 BTC
Bob pays Alice 10 BTC

History

- Bitcoin was created in 2009 by someone known as Satoshi Nakamoto.
- Does not require the support of a central government or organisation to regulate it, nor a broker to manage payments.
- The Bitcoin currency is instead created when users *mine* for it, using their computers to perform complex calculations through special software.
- Bitcoin (BTC) divisible to the 8th decimal place.
- BTC can be split into 100,000,000 units.
- 0.00000001 bitcoin is one Satoshi.

History

- Bitcoin designed to limit the number of bitcoins that can ever be created.
- Each transaction then has a reward, and the reward reduces over time, which should reduce the supply of the coins.
- In 2016, the reward for a successful mining process was reduced from 25 BTC to 12.5 BTC. This reward will continue to reduce until the currency is forked (and where new parameters are used), or when we reach a saturation level.
- Others: Ethereum, Ripple, Litecoin, Monero, Ethereum Classic, Dash, Steem, KiloCoin and Augur.

Genesis Record

Summary	
Height	0 (Main chain)
Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Previous Block	0000000000000000000000000000000000000000000000000000000000000000
Next Blocks	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Time	2009-01-03 18:15:05
Difficulty	1
Bits	486604799
Number Of Transactions	1
Output Total	50 BTC
Estimated Transaction Volume	0 BTC
Size	0.285 KB
Version	1
Merkle Root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
Nonce	2083236893
Block Reward	50 BTC
Transaction Fees	

4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b 2009-01-03 18:15:05

No Inputs (Newly Generated Coins) → 1A1zP1eP5QGefi... (Genesis of Bitcoin) 50 BTC

50 BTC

Big accounts

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r
Hash 160	7c6775e20e3e938d2d7e9d79ac310108ba501ddb
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	3493
Total Received	1,210,471.32658275 BTC
Final Balance	180,773.05403806 BTC

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	3EDzR4QKeGJyCZWXMF1kAGqi8gHNQ798sF
Hash 160	897d25262f68b8a8d4e2adf2ab082ce0f58a69d1
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	1
Total Received	2,034.668943 BTC
Final Balance	2,034.668943 BTC

Request Payment

Donation Button

e3a9cbec0c5ec55db3ac02029d8cbaf1370e04e8603d9e5000106091c66c308d 2017-11-14 08:03:03

3Qk9qheSn4Y5wUCmSAT4ggbhHbRRgRdVaW	1LAGK834p9y4h34jWgGjHsSRNUgKWB9Cho	0.009 BTC
	1GANRvqWMg1zmVGU2WKUAuGDS5PGj3KBNx	0.01718 BTC
	3Mfiy7hJB44kY7YHRgCuJ7JgpzuL1tSqWg	15.6262 BTC
	37kTvhCNe8WmLnhdjBRRZBtEL5zzH94Zq8	0.31678 BTC
	1FKjowv879X5RGDeU21zzxinVbgNoeGaHr	0.169 BTC
	3BazbNWURUzdk58myGn1V9F6HPabtUjZwN	0.01265 BTC
	3HCJDcEjzHyip6TJ3kwQQaJGxJW6scbzGB	13,067.17305362 BTC

13,083.32386362 BTC

Genesis Record

Summary	
Address	3EDzR4QKeGJyCZWXMF1kAGqi8gHNQ798sF
Hash 160	897d25262f68b8a8d4e2adf2ab082ce0f58a69d1
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	1
Total Received	2,034.668943 BTC
Final Balance	2,034.668943 BTC

Request Payment

Donation Button

Transactions (Oldest First)

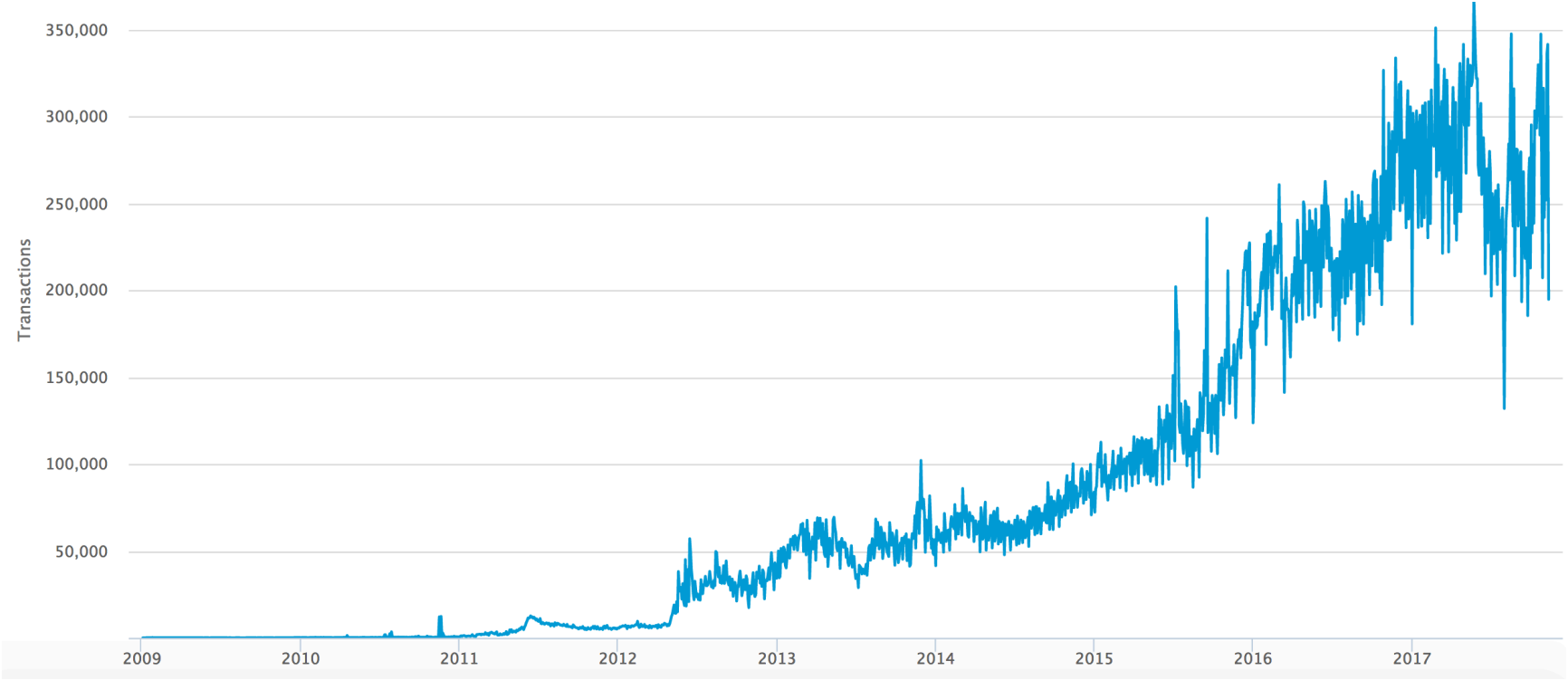
Filter

67079f670818b0e44ed70399bcdc4664a8595fb6f90f8538b7821c7ac889bbe8			2017-11-13 19:10:37
3HomPY371CsvvjyaCZj7ExLf1TcSQ82HuG	→	3EDzR4QKeGJyCZWXMF1kAGqi8gHNQ798sF	2,034.668943 BTC

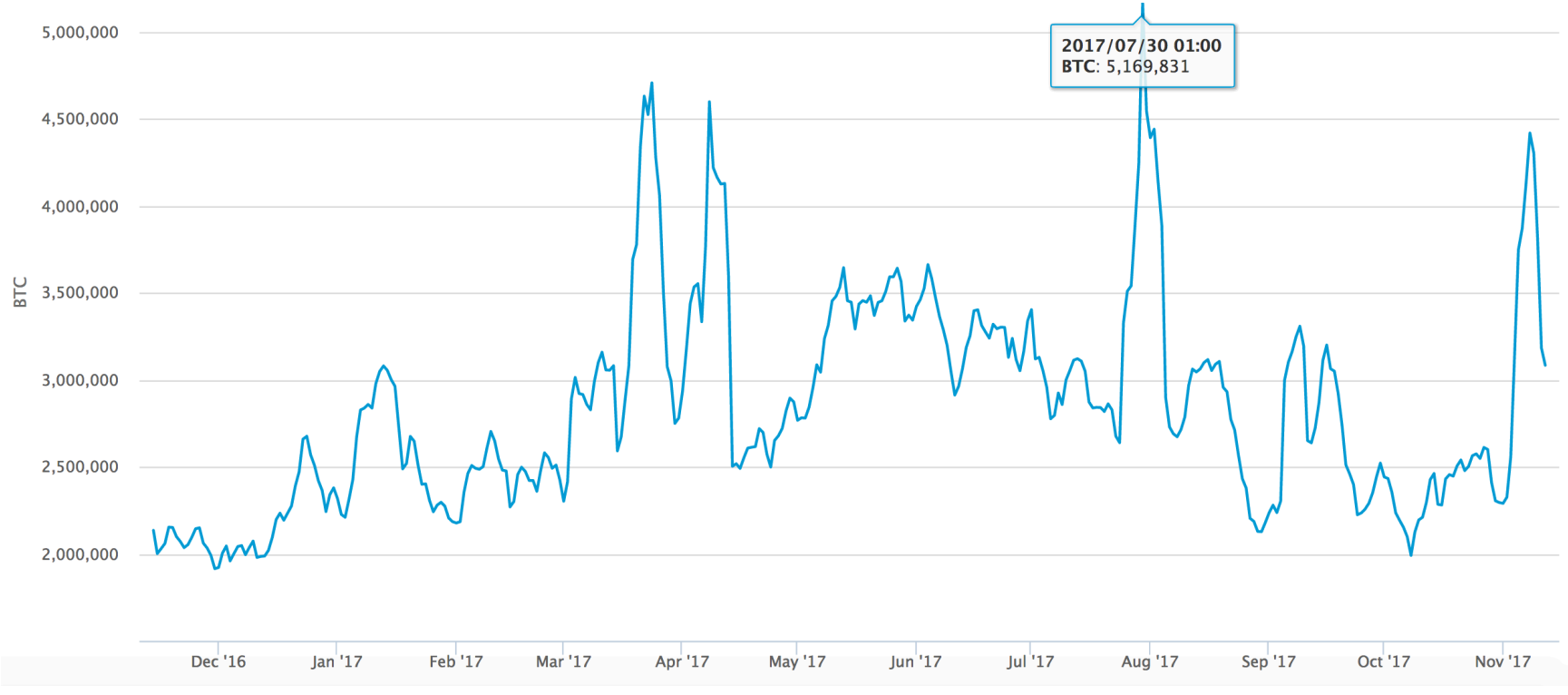
1 Confirmation

12,801,546.94 USD @2017-11-13T19:10:37Z

Bitcoin transactions

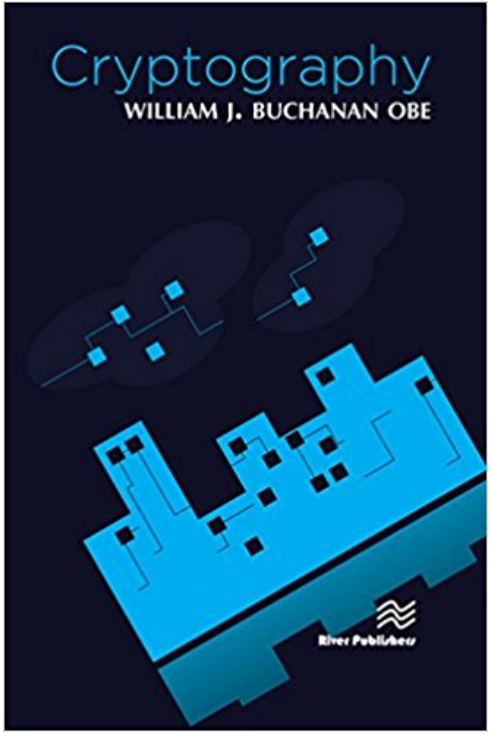


Bitcoin trading volume



Bitcoin value

Chapter 10: Blockchain and Cryptocurrencies

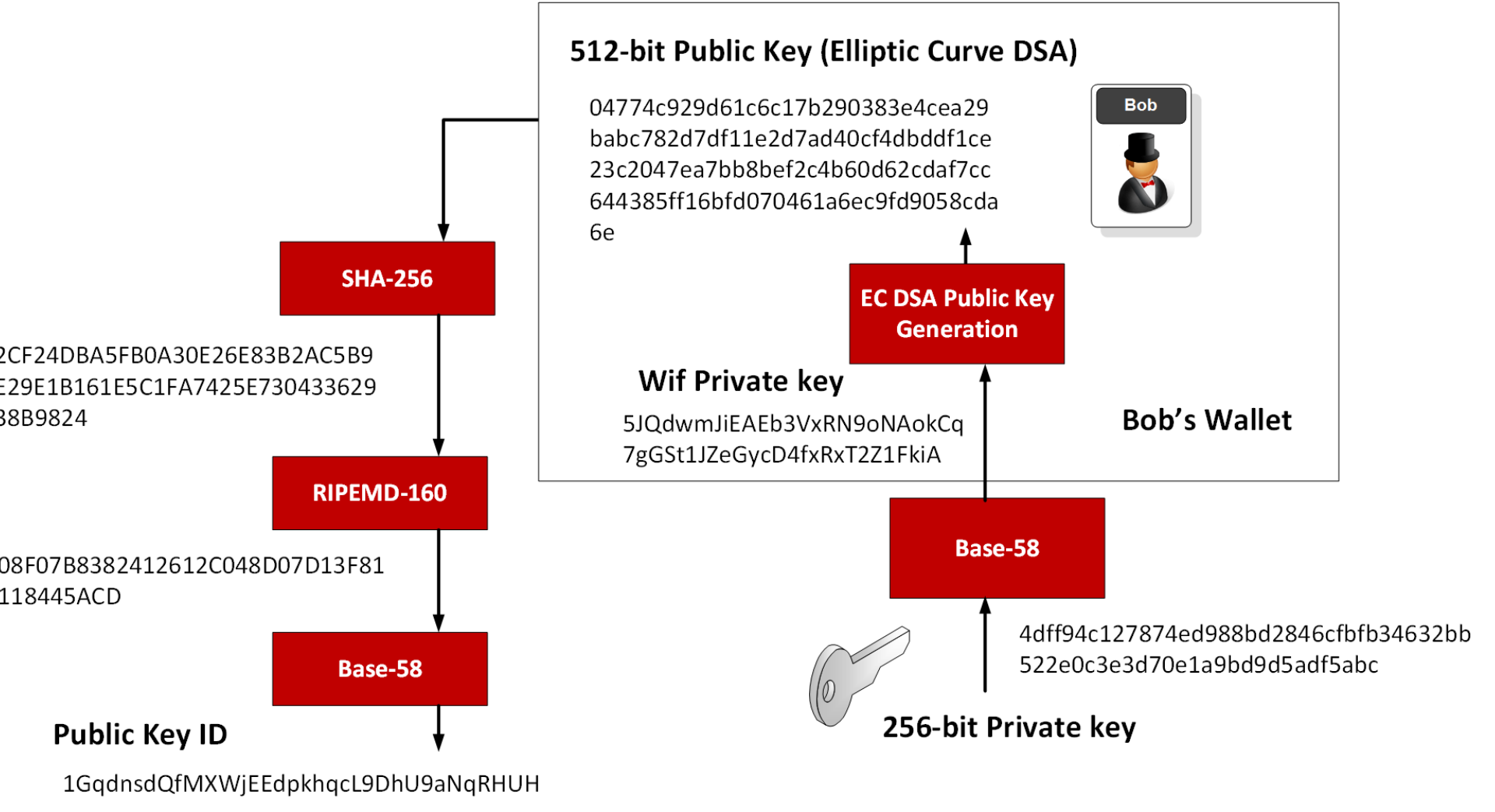


Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts

Prof Bill Buchanan OBE

http://asecuritysite.com/crypto10
http://asecuritysite.com/encryption

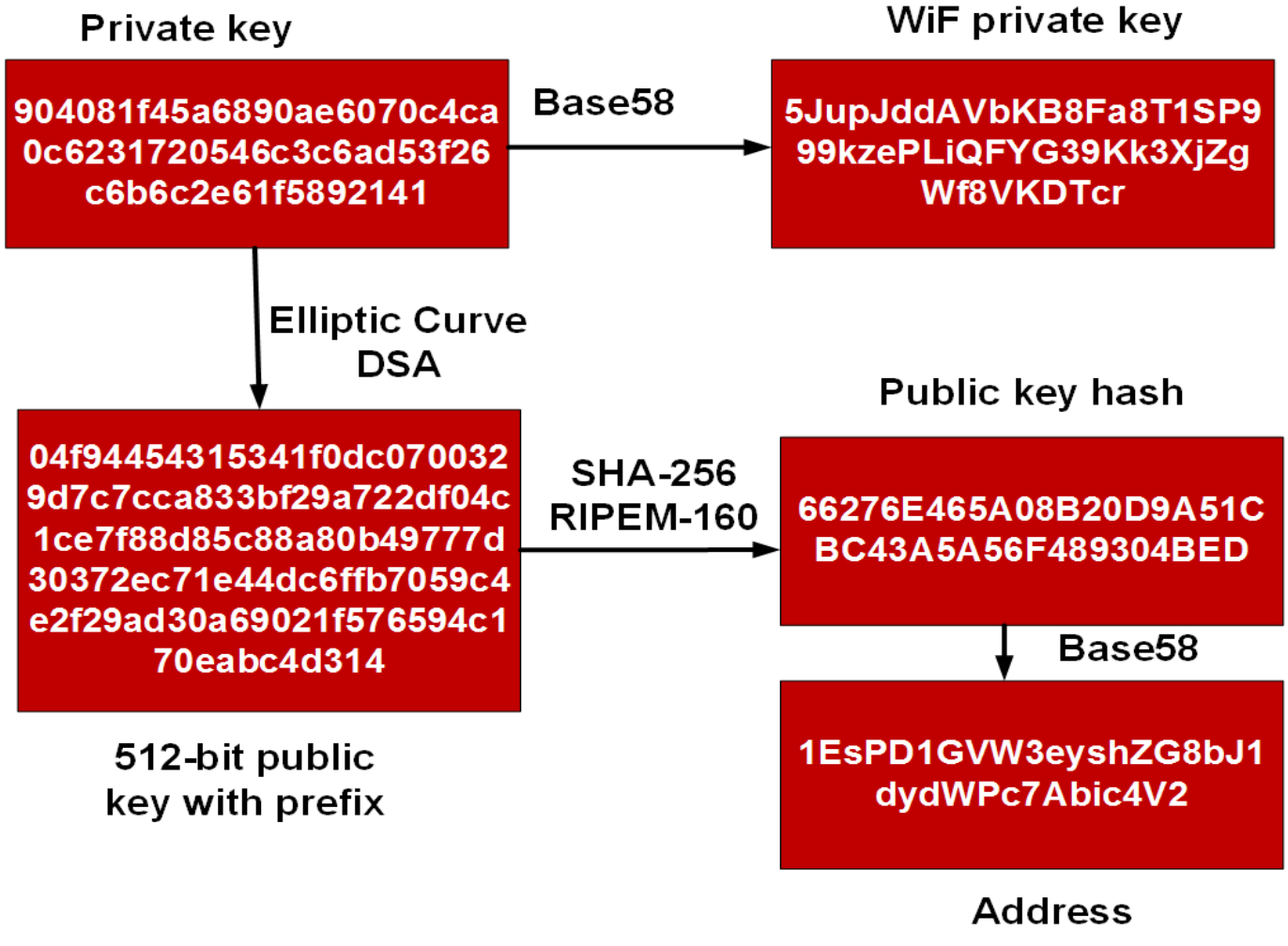
Bitcoin Wallet and Addresses



Summary	
Address	1JyvJ5TcN2hzu7dDEeVuuikgyHtpwU8NE6
Hash 160	c53deb8dda6fb0c388da19fbcf63270cc4f4cbfd
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	20
Total Received	0.64531495 BTC
Final Balance	0 BTC

Request Payment | Donation Button


Private key
904081f45a6890ae6070c4ca0c6231720546c3c6ad53f26c6b6c2e61f5892141
Base58
WiF private key
5JupJddAVbKB8Fa8T1SP999kzePLiQFYG39Kk3XjZgWf8VKDTcr
Elliptic Curve DSA
04f94454315341f0dc0700329d7c7cca833bf29a722df04c1ce7f88d85c88a80b49777d30372ec71e44dc6ffb7059c4e2f29ad30a69021f576594c170eabc4d314
512-bit public key with prefix
SHA-256 RIPEM-160
Public key hash
66276E465A08B20D9A51CBC43A5A56F489304BED
Base58
1EsPD1GVW3eyshZG8bJ1dydWPc7Abic4V2
Address

Private key:
4c0333a50b7724c71b89df148d83f64d49d896e21701007eeb8cada52744aca2

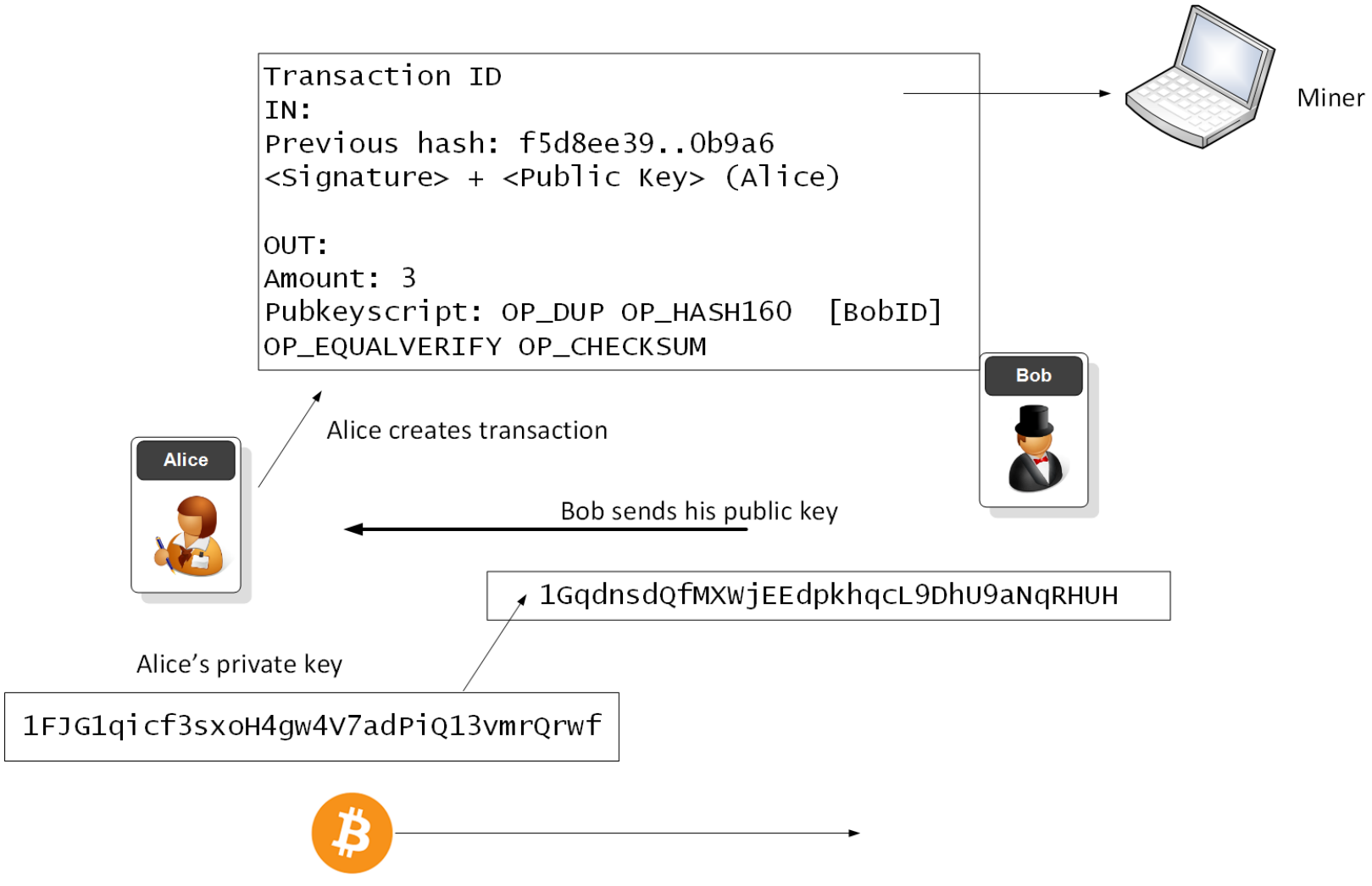
Public key:
0489fc7b8c3f655a10840d35c76ebb5596694045e49e940fb1e7a759da4edf0fafc45b
bbea6f5a56abf14c145c529c8eda9d3ad606f3a0bf4ca01ce991d4987b97

Wif: 5JPmDetQXXvc5aT5efyrg7BxHbH4135owRzq9DD7n2eWQCta5MN

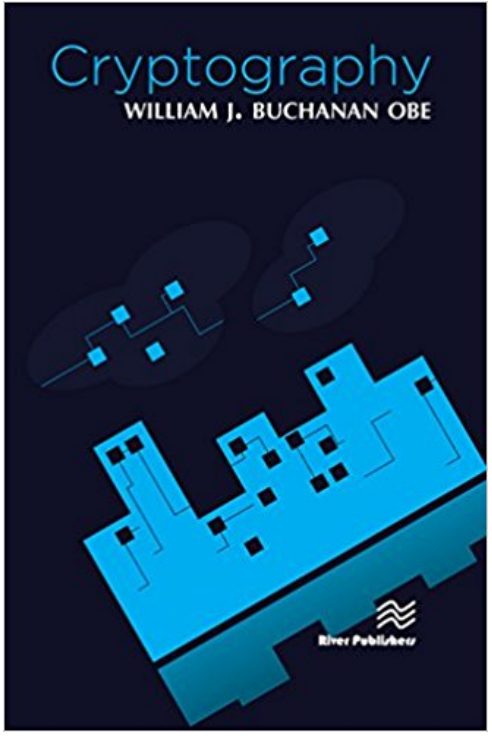
Address: 16RAf9CjnstWCfBJGfrzSSMfTeHJVt8QWw

Signed:
483045022026 4c4dce5f1cf0dff8d32d21c5d5cf6baed428b12ae6f8594924246a611e
9ee602210096ef8e7054ec7a39f0a35d8de3fd50090b1d125c0e795af8cf3d577b676
407ca01410489fc7b8c3f655a10840d35c76ebb5596694045e49e940fb1e7a759da4e
df0fafc45bbbea6f5a56abf14c145c529c8eda9d3ad606f3a0bf4ca01ce991d4987b97

Bitcoin transaction



Chapter 10: Blockchain and Cryptocurrencies

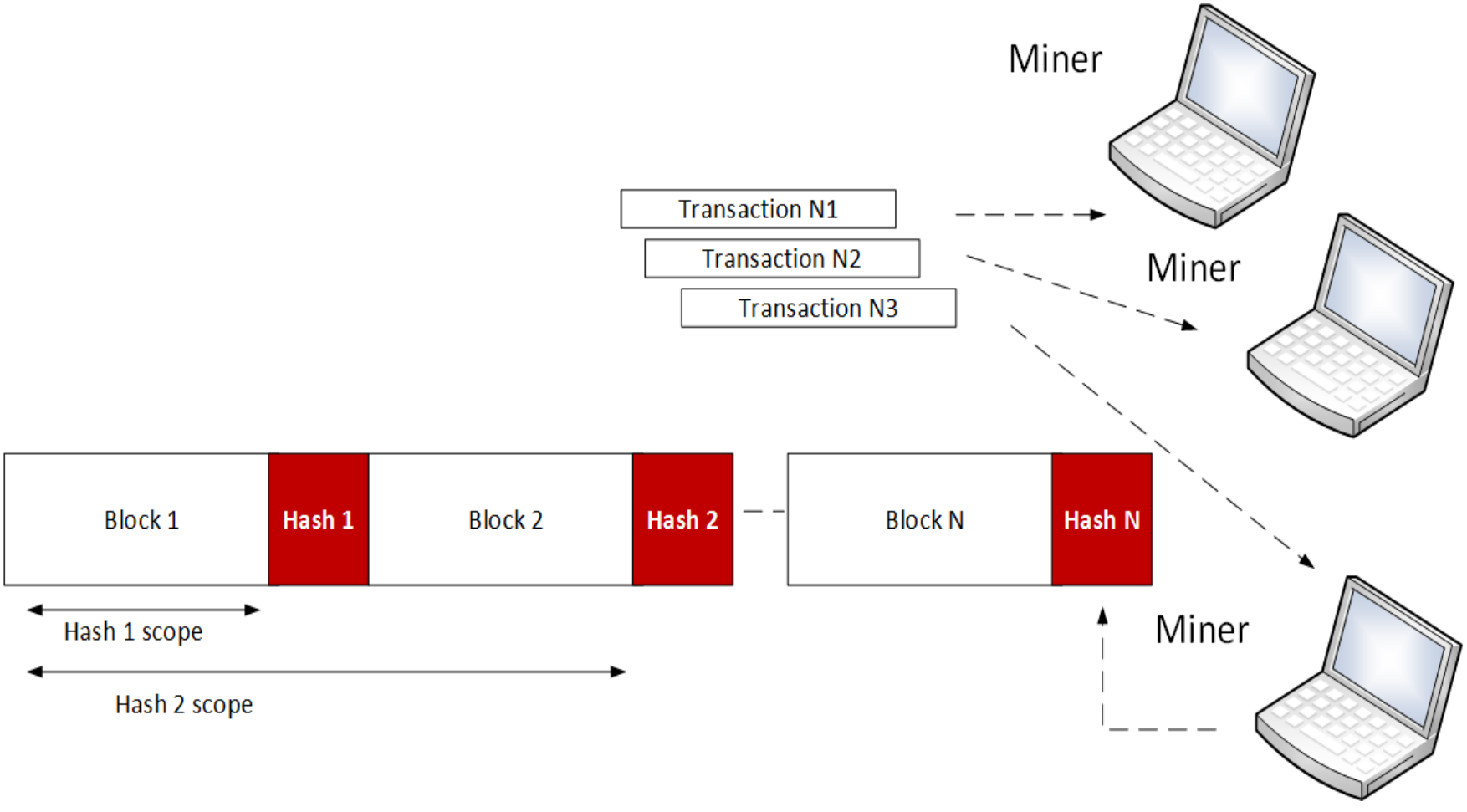


Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts

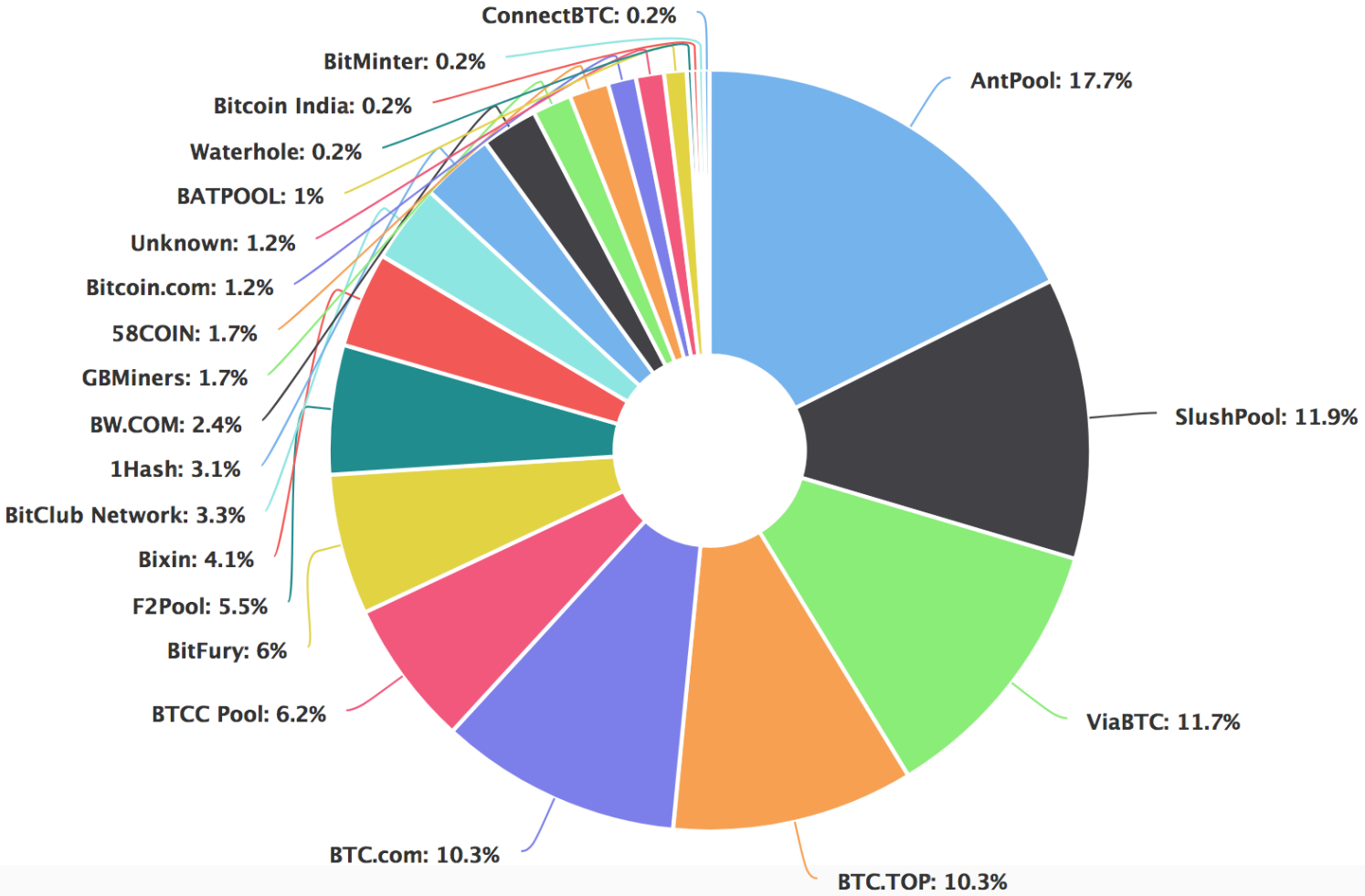
Prof Bill Buchanan OBE

http://asecuritysite.com/crypto10
http://asecuritysite.com/encryption

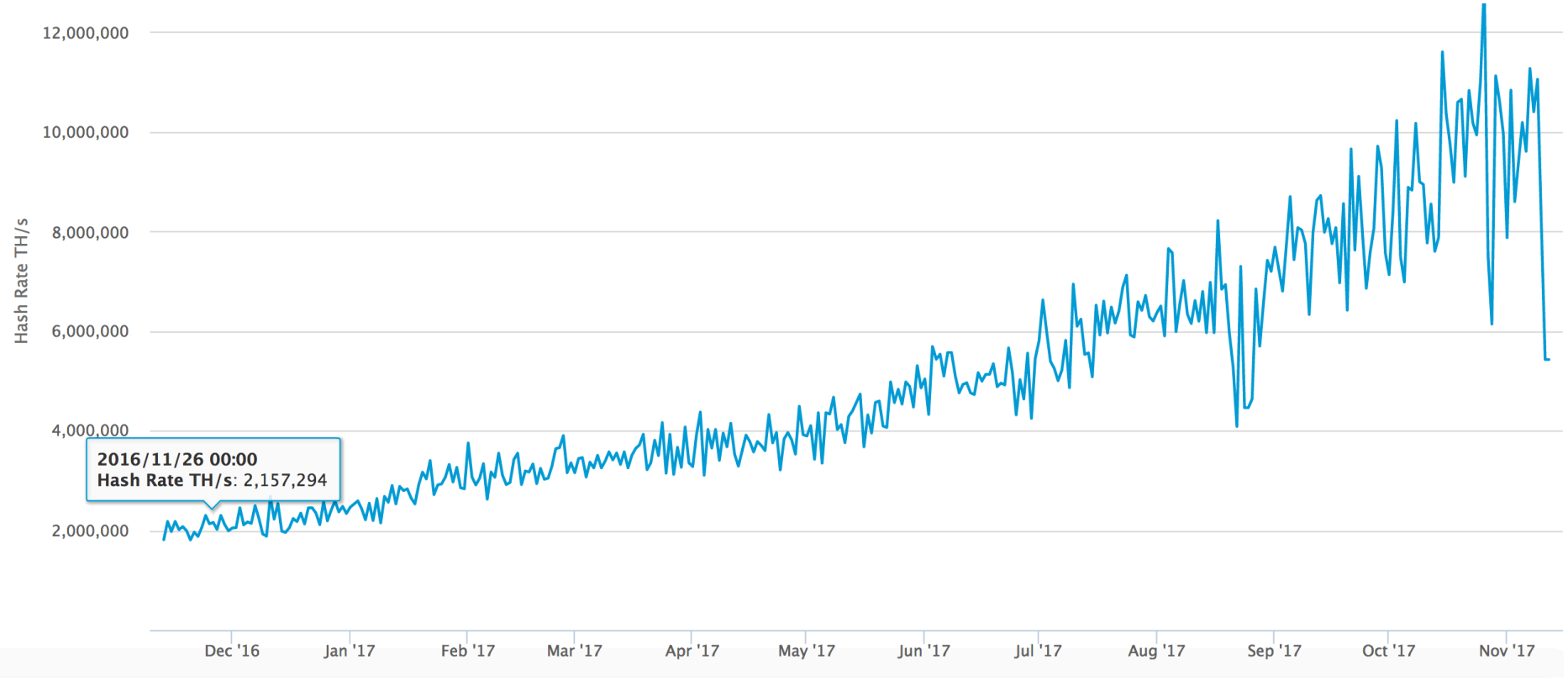
Mining process



Successful miners



Hash Rate TH/s



Mining Processes

- Hash
- 0000000000000000d98e57b83834a2d1f4387a93d06861bcf3ea5fc498bd55
- Previous Block
- 0000000000000000012138e05f0779765277a9d2ab7e4a2a70882790abf98a0c

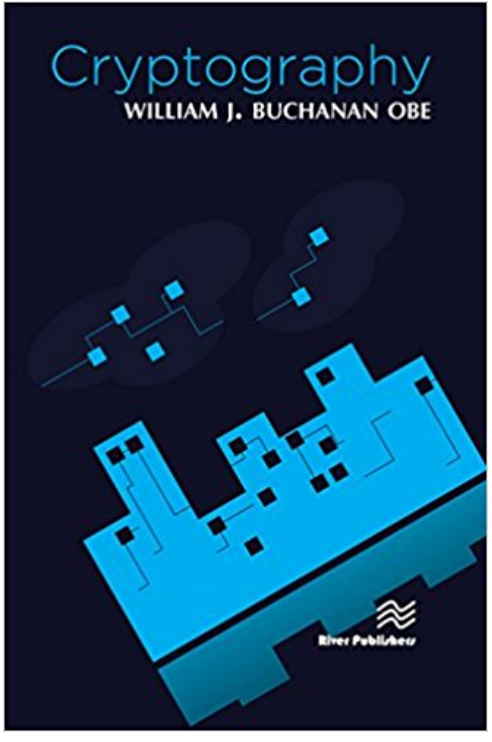
Blocks

Block #475370

Summary	
Number Of Transactions	1937
Output Total	10,443.01703436 BTC
Estimated Transaction Volume	555.96160374 BTC
Transaction Fees	0.87013657 BTC
Height	475370 (Main Chain)
Timestamp	2017-07-11 21:44:58
Received Time	2017-07-11 21:44:58
Relayed By	AntPool
Difficulty	708,659,466,230.33
Bits	402754864
Size	998.17 KB
Version	0x20000000
Nonce	1203121562
Block Reward	12.5 BTC

Hashes	
Hash	00000000000000000d98e57b83834a2d1f4387a93d06861bcf3ea5fc498bd55
Previous Block	00000000000000000012138e05f0779765277a9d2ab7e4a2a70882790abf98a0c
Next Block(s)	00000000000000000010e3117695c04d66d31cfa8489b70579dcc2f12c5a2daae
Merkle Root	140d91abab9501d50ace079ba12c80125f48c2b5fe7d9da685ea3ee8ea767e82

Chapter 10: Blockchain and Cryptocurrencies



Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts

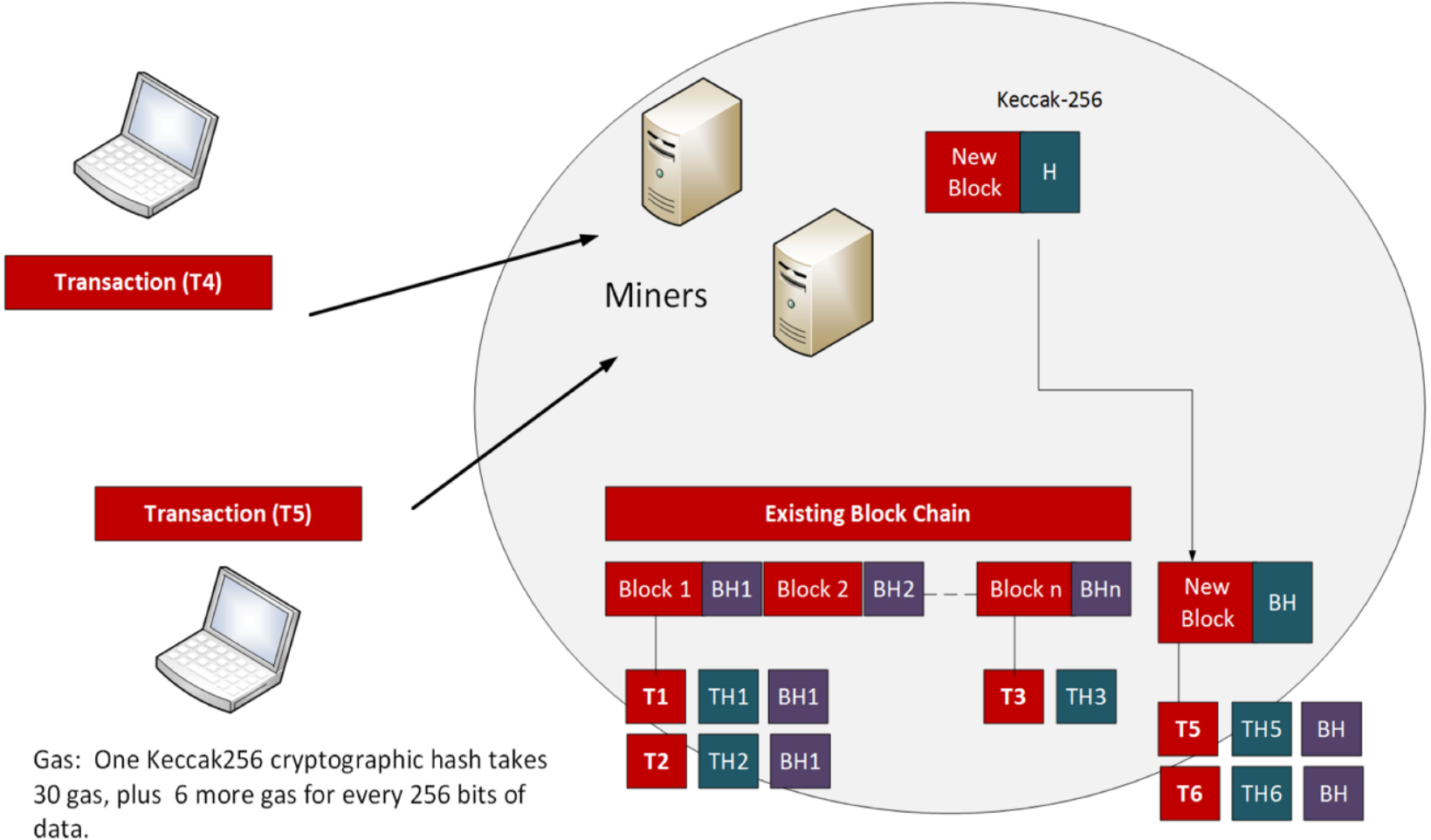
Prof Bill Buchanan OBE

http://asecuritysite.com/crypto10
http://asecuritysite.com/encryption

History

- Ethereum was created by Vitalik Buterinin in 2015 and which built on the Bitcoin/ Blockchain concept by included the concept of smart contracts.
- After a hack, in 2016, the Ethereum currency split into two: Ethereum (ETH) and Ethereum Classic (ETC).

Ethereum setup



Gas: One Keccak256 cryptographic hash takes 30 gas, plus 6 more gas for every 256 bits of data.

Gas

- Within Ethereum applications we define the concept of *gas*. This is basically the unit that is used to measure the amount of work that is required to perform a single Keccak-256 hash, and where 30 gas are consumed for a single hash and 6 more gas for each 256 bits of data hashed. In this way there is a motivation to keep contracts small, as they will be less costly.

Gas

- Gas thus provides a way to define the fee that miners receive in performing operations on the blockchain.
- This differs from Bitcoin which only charges for the number of kiloBytes in a transaction. When it comes to the actual payment of the transaction fees, there is a payment of ether to the miners who create the blocks.

Gas

- Ethereum transactions thus have a fee associated with them. If the fee is too low, then the miners will not process the transaction.
- When gas is consumed it is paid to the miner, and cannot be recovered back.
- If the transaction fee is set too high, there are likely to be many eager miners who are keen to profit from the high fee, and your transaction is likely to be prioritized.

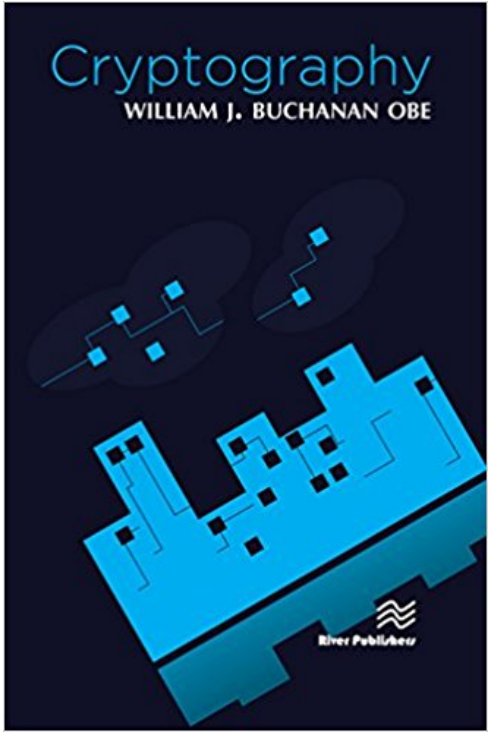
Gas

- Overall, though, miners only charge for the work they have done, and they will return back any excess gas which they have not used. A miner can decide whether it needs to change the use of gas according to the price of gas varying. This overcomes the changes in transaction fees that happen in Bitcoin.

Gas

- In Ethereum, just like Bitcoin, there is a block limit, so you'll end up paying more if you overspill into another block (which means you should be efficient with your code and data).
- The gas price per transaction aims to overcome denial of service and infinite loops, and where 0.00001 Ether or 1 Gas is used to execute a line of code. If there is not enough Ether, no transaction will be performed. It also aims to make code designers efficient and not use waste bandwidth and CPU utilization.

Chapter 10: Blockchain and Cryptocurrencies

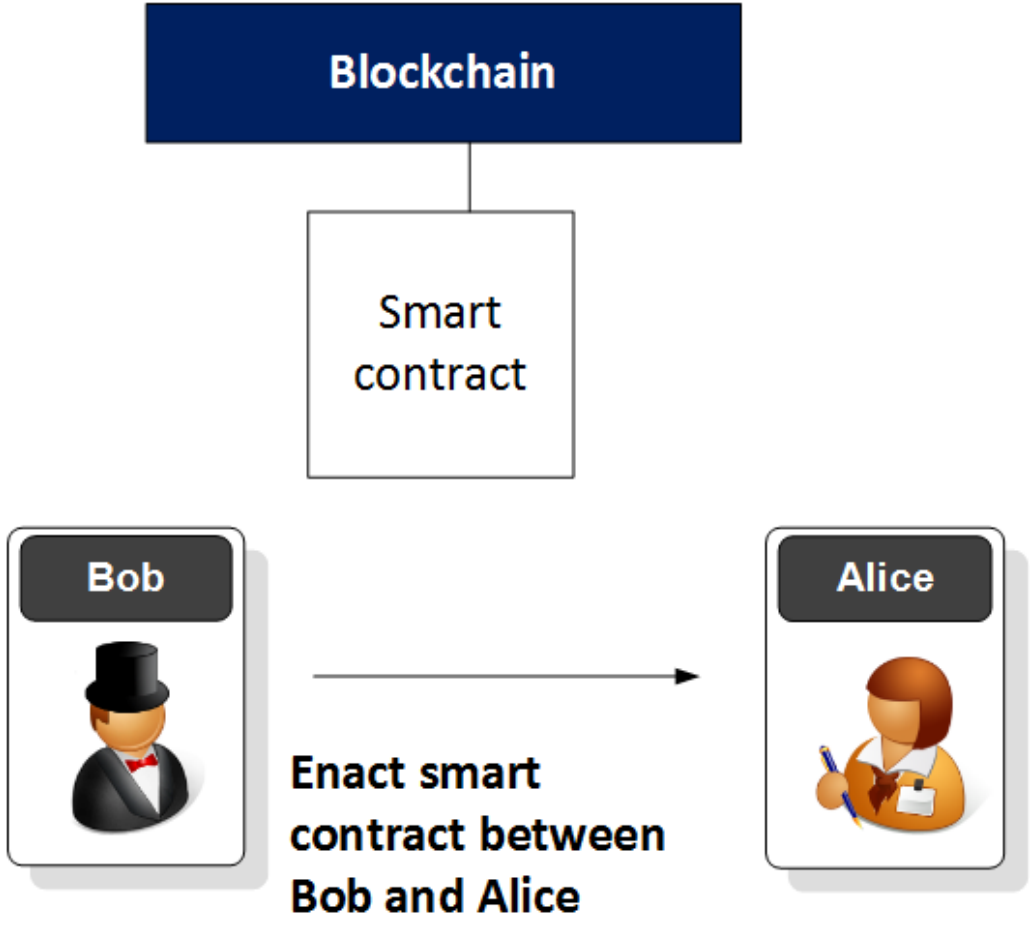


Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts

Prof Bill Buchanan OBE

http://asecuritysite.com/crypto10
http://asecuritysite.com/encryption

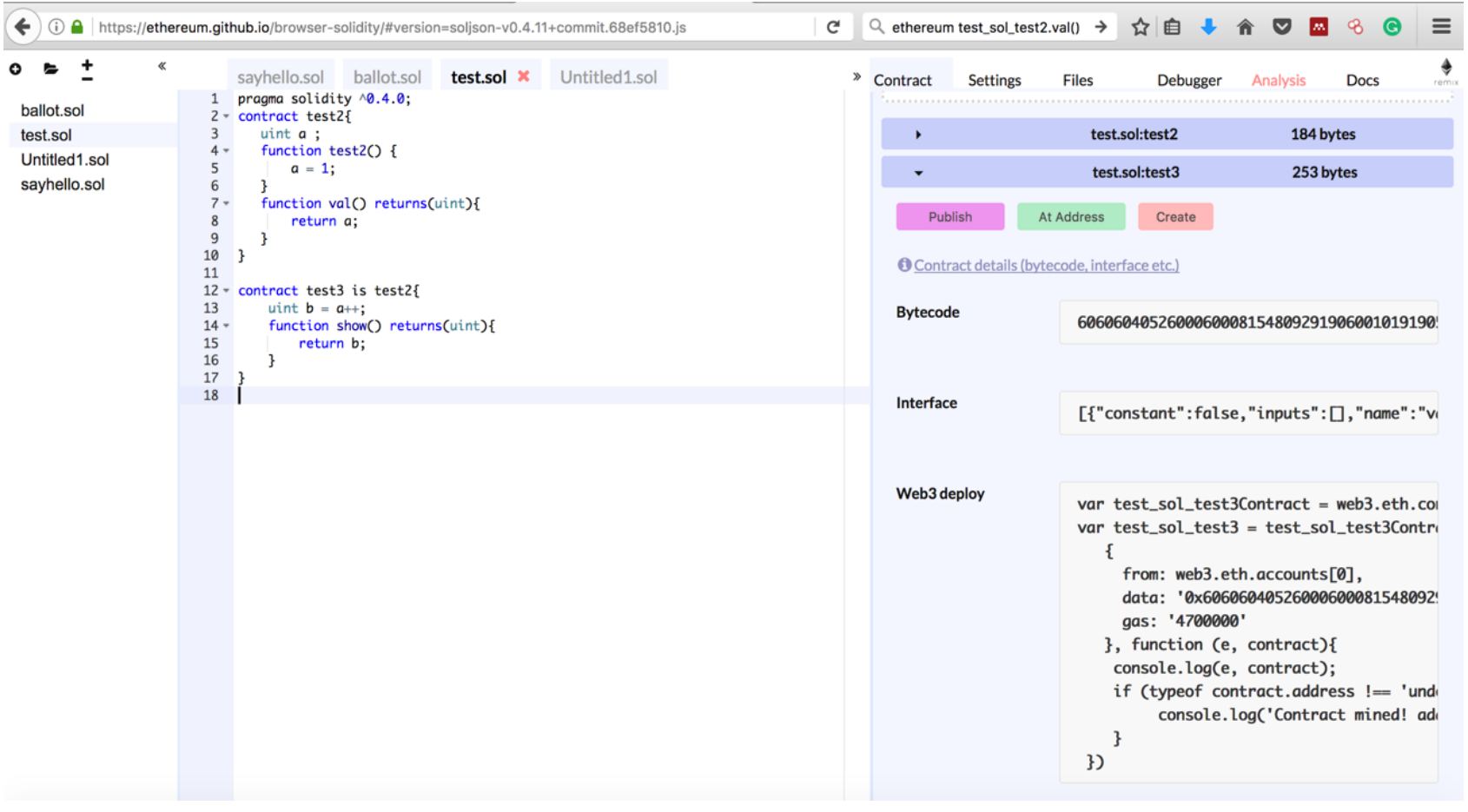
Smart Contract



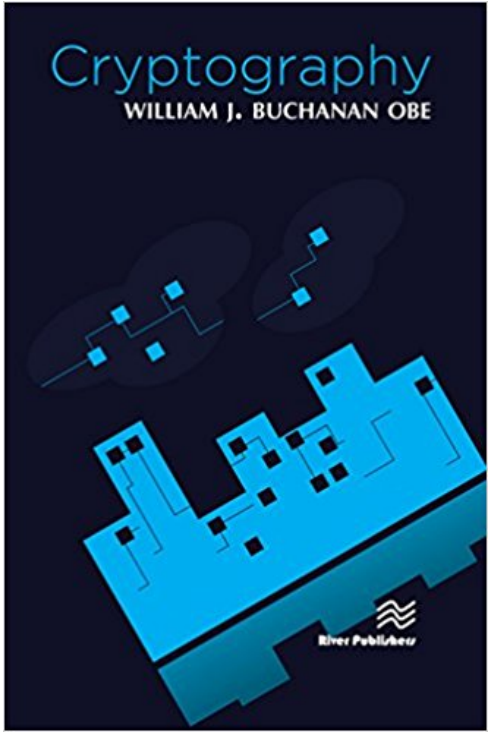
```
pragma solidity ^0.4.0;
contract test2{
   uint a ;
   function test2() {
      a = 1;
   }
   function val() returns(uint){
      return a;
   }
}

contract test3 is test2{
    uint b = a++;
    function show() returns(uint){
       return b;
    }
}
```

Compile with Solidity



Chapter 10: Blockchain and Cryptocurrencies



Cryptocurrencies
Bitcoin addresses
Blockchain
Mining
Ethereum
Smart Contracts

Prof Bill Buchanan OBE

http://asecuritysite.com/crypto10
http://asecuritysite.com/encryption