Your World First

C/M/S/
Law.Tax

Blockchain in a day

GDPR and Blockchain

Introduction: me

Results	
Original text	Simon Sanders
Original bytes	53:69:6d:6f:6e:20:53:61:6e:64:65:72:73 (length=13)
Adler32	21da04f7
CRC32	017e4392
Haval	fc9907a9d8490ae709a98ec39ede0a04
MD2	450341047e391ab7107c6255a0f0984f
MD4	8aa510cfcde137ac3277948d79ed4005
MD5	75a2c0cd6ba8a9f146587be8f52c03b1
RipeMD128	3e8826d22191fe95db3e1a29bd4d89a6
RipeMD160	871db23852b2b81c36464e4cb10a620ba0253c2f
SHA-1	d8d41943537ef6a0007ee880668c06c3c1d627e1
SHA-256	6cb04d8655f64525a51ddd8f3b0c50180bac45ede54da8808301778fa872a08e
SHA-384	6e09ef491e6a40a7712b32917eb94641331929099a18def31e5de815a0fd1edd32907c5bfec34ae5dceee95316baf9b9
SHA-512	93d4e8fd1bab46ed6e8407cbf4020f265d30f6208ca6fc058d22d4ee4d9725e42193d8e5902e3797c8da711aac2523369b9bc01b50bacdb880d02fd5037c33e8
Tiger	3e6ee56b59a65118648f2af622d1c5388be7d99477eb3c28
Whirlpool	fd28eff9ff01f363b1ecc558fe2d8eb773c9c9f46c22cfe7798b4962643d37450c287a06d57021e39f9a500ffde59f04b4e33caec380c6852f2169e9cef278fb

Used: https://www.fileformat.info/tool/hash.htm

Introduction

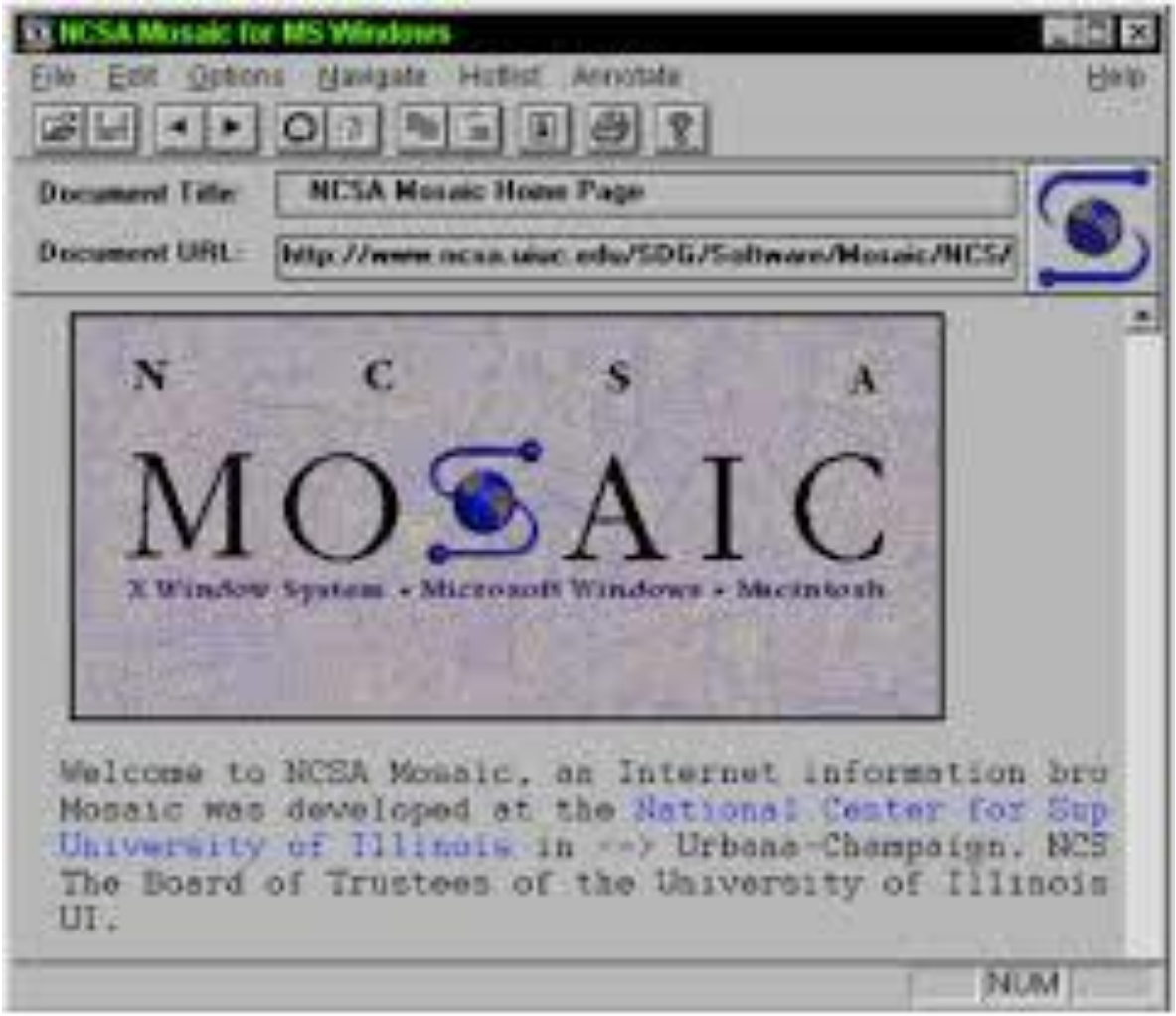
- Blockchain and GDPR, complicated subjects in isolation, let alone if discussed in conjunction;
  - They are two areas in development
  - Assumption for today: GDPR as a relative constant and Blockchain as variable
  - Today will be about understanding the driving principles of Blockchain and to compare those with the driving principles of the GDPR

Introduction: Today

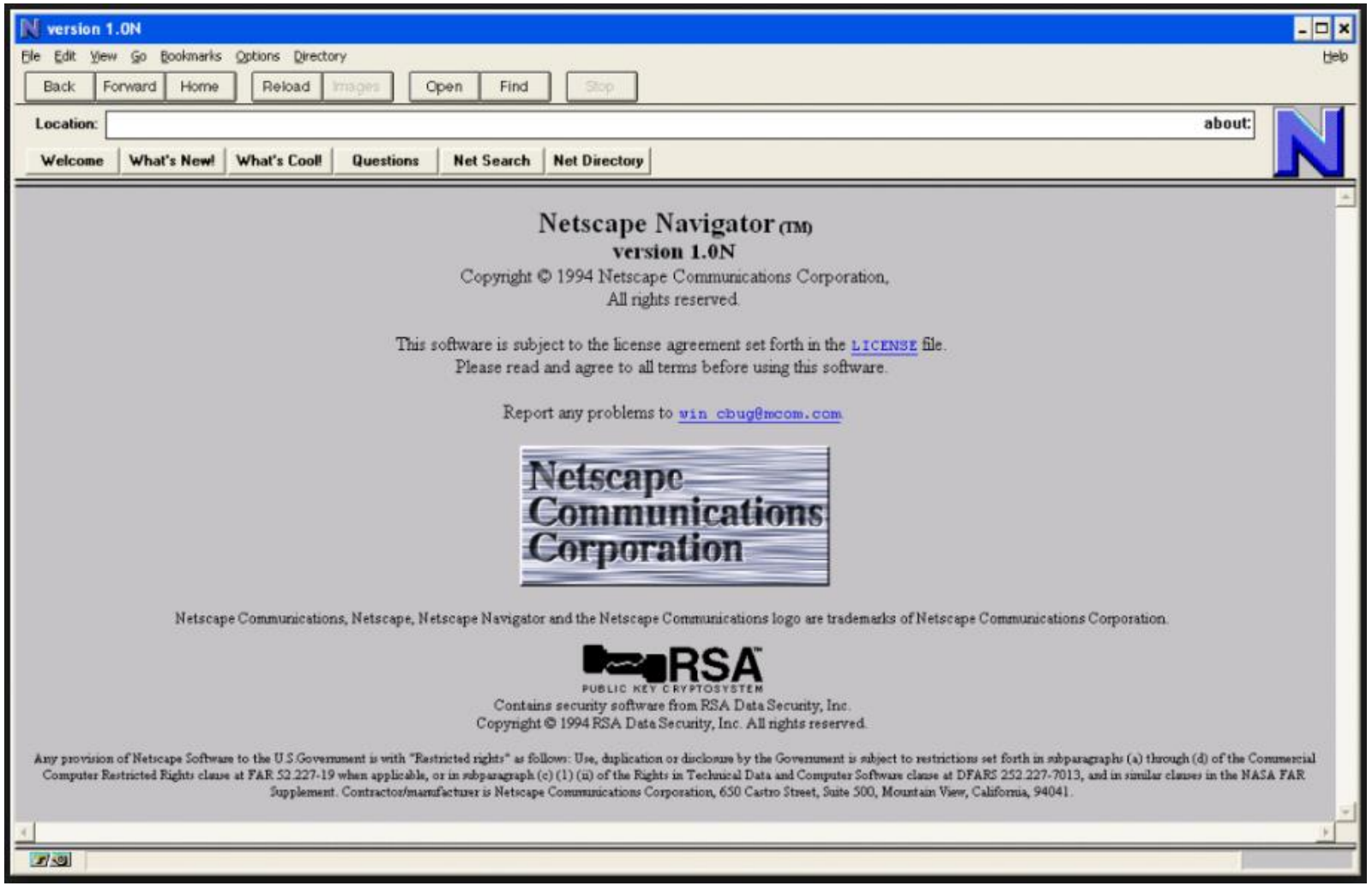
A structured approach;

1. Historic background in summary
2. Explanation of:
   a) GDPR
   b) Blockchain
3. Identifying potential GAP’s
4. Some observations
5. Question time

Background of the GDPR



Background of the GDPR



Background of the GDPR

- GDPR as (*inter alia*) a response to rapid technological developments and globalisation (R6).

- Reading between the lines: more and more personal data processed in a sometimes poorly controlled environments, so boundaries had to be set / beefed up.

- One of the aims: provide better means of control over personal data which is acquired by (centralised) organisations, to data subject.

- Key word: accountability, but directed at (centralised) organisations and centralised data structures.

Background Blockchain

In summary as Wikipedia has summarised it as:

- Blockchain was invented by Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin.
- The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server.

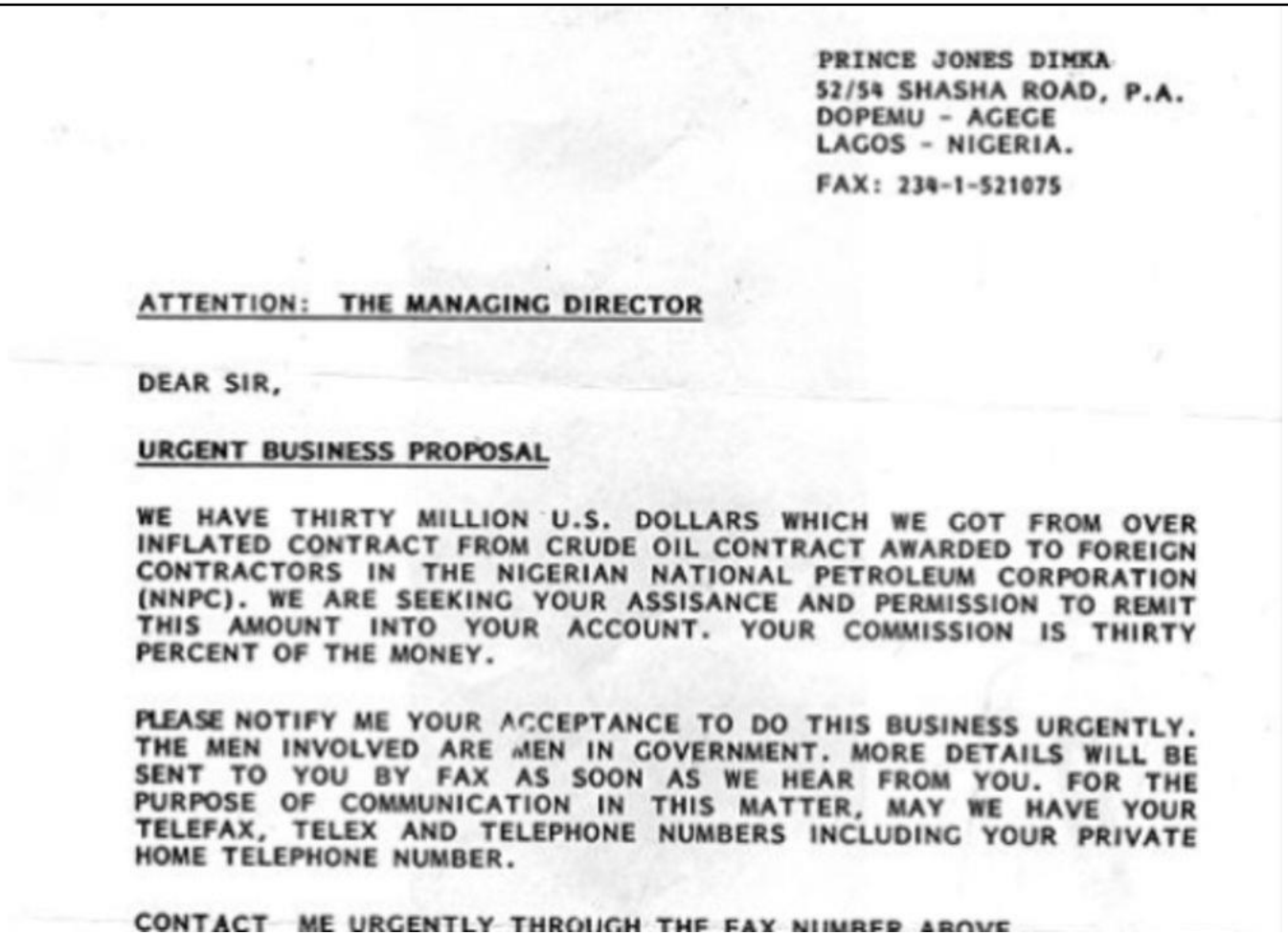
- Comparable to GDPR considerations: take control back from central organizations who may abuse power or violate trust.

It is all about trust (or lack thereof)

I

It is all about trust (or lack thereof)

I



PRINCE JONES DIMKA
52/54 SHASHA ROAD, P.A.
DOPEMU - AGEGE
LAGOS - NIGERIA.
FAX: 234-1-521075

ATTENTION: THE MANAGING DIRECTOR

DEAR SIR,

URGENT BUSINESS PROPOSAL

WE HAVE THIRTY MILLION U.S. DOLLARS WHICH WE GOT FROM OVER INFLATED CONTRACT FROM CRUDE OIL CONTRACT AWARDED TO FOREIGN CONTRACTORS IN THE NIGERIAN NATIONAL PETROLEUM CORPORATION (NNPC). WE ARE SEEKING YOUR ASSISANCE AND PERMISSION TO REMIT THIS AMOUNT INTO YOUR ACCOUNT. YOUR COMMISSION IS THIRTY PERCENT OF THE MONEY.

PLEASE NOTIFY ME YOUR ACCEPTANCE TO DO THIS BUSINESS URGENTLY. THE MEN INVOLVED ARE MEN IN GOVERNMENT. MORE DETAILS WILL BE SENT TO YOU BY FAX AS SOON AS WE HEAR FROM YOU. FOR THE PURPOSE OF COMMUNICATION IN THIS MATTER, MAY WE HAVE YOUR TELEFAX, TELEX AND TELEPHONE NUMBERS INCLUDING YOUR PRIVATE HOME TELEPHONE NUMBER.

CONTACT ME URGENTLY THROUGH THE FAX NUMBER ABOVE

So who do you trust?

So who do you trust?

So who do you trust?

So who do you trust?

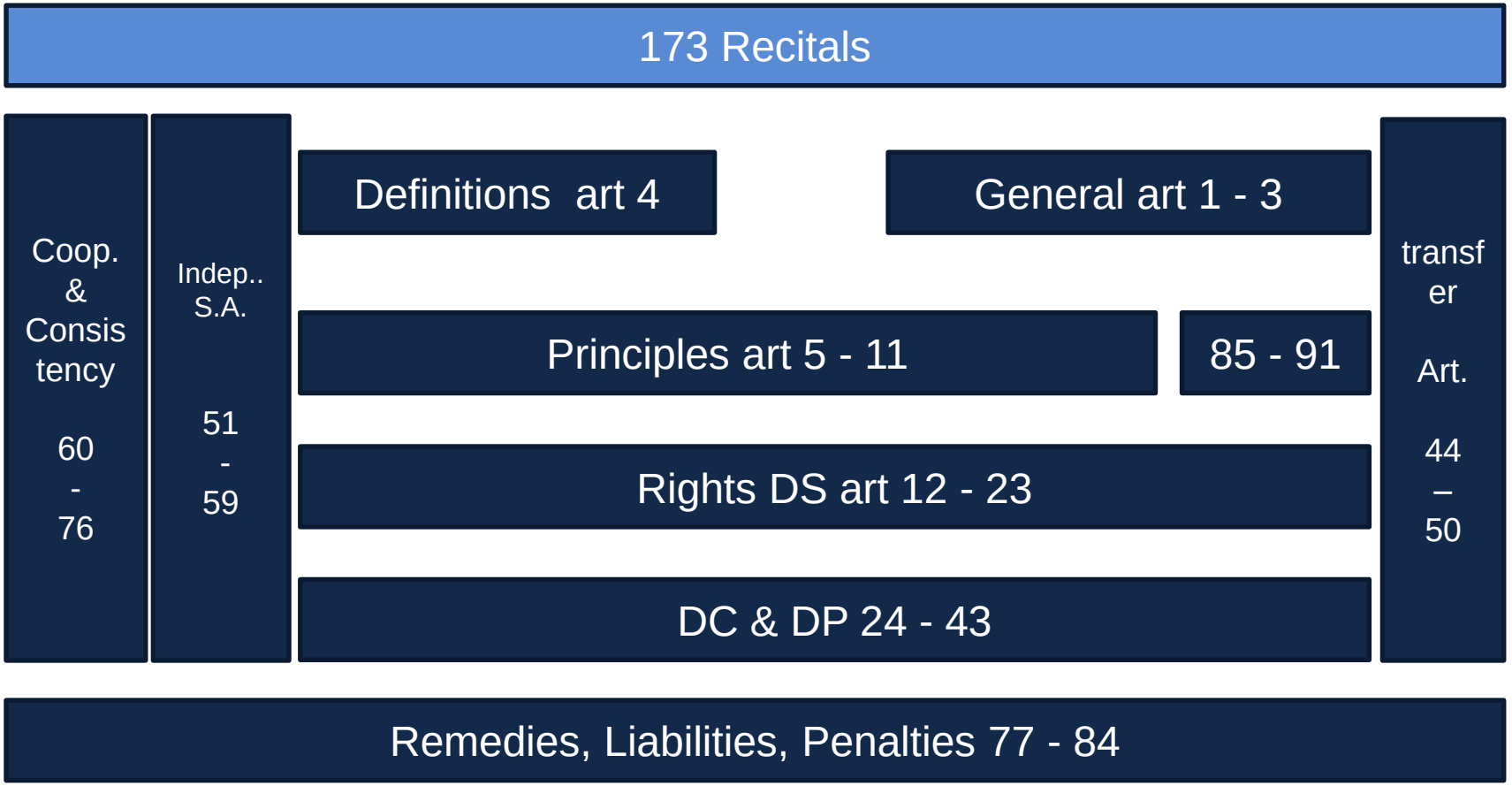
So who do you trust?

So who do you trust?

So who do you trust?

Lets ask the GDPR whom to trust

Structure GDPR



The GDPR

For today, we need to consider the below consecutive steps:

1. Is the GDPR applicable (territorial scope, art 3 GDPR)
2. What data is considered PD (article 4, definition PD and processing)
3. If data is considered PD, then processing is only lawful if based on one of the grounds set out in article 6 GDPR
4. And applying those principles as set out in article 5 (1) of the GDPR (broad principles)
5. While respecting the rights of the DS (12 – 23 GDPR)
6. And implementing those obligations as set out for the DC or DP (24 – 43 GDPR)

It is as simple as that.

The GDPR

What data is considered PD (definition PD + processing)

Personal data *means any information* ***relating to*** *an identified or identifiable natural person ('data subject');*

an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

The GDPR

What data is considered PD (definition PD + processing)

Processing *means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as;*

collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The GDPR

If data is considered PD, then processing is only lawful if based on one of the grounds set out in article 6 (1) GDPR;

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Or 6 (4) … (in summary) compatible with the purpose for which the data are initially collected.

The GDPR

And applying those principles as set out in article 5 (1) of the GDPR (broad principles)

a) Lawfulness, fairness and transparency
b) Purpose limitation
c) Data minimization
d) Accuracy
e) Storage limitation
f) Integrity and confidentiality

The GDPR

While respecting the rights of the DS (12 – 23 GDPR)

a) Transparency, communications (12)
b) Information on personal data obtained from DS (13)
c) Information on personal data obtained from third parties (14)
d) Right of access of DS to personal data (15)
e) Right to rectification (16)
f) Right to erasure (right to be forgotten) (17)
g) Right to restriction of processing (18)
h) Notification obligation of DC (19)
i) Right to data portability of DS (20)
j) Right to object and automated decision making (21)
k) Automated decision making (22)

The GDPR

And implementing those obligations as set out for the DC or DP (24 – 43 GDPR)

Determines purpose and means of processing (alone or jointly)

a) General: take measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR
b) Data protection policy
c) Data protection by design and default
d) Appoint representative in Union (27)
e) If data processor is engaged, -> agreement and safeguards
f) Records of processing activities (30)
g) Security of personal data (33), notification/comm's of breach (34, 35)
h) DPIA, DPO, Code of conduct, Certification (36 – 43)

The GDPR

Remember: the point of accountability in the GDPR is with the DC!

It is the person, persons organisation or organisations that sometimes jointly determine purpose and means of the processing.

The GDPR is not addressed to the maker of the software!

The GDPR

So in summary:

1. If data is personal data (keep reading that definition in 4)
2. And there is a valid legal basis for processing (choice of 6, read in 6)
3. Apply all 6 principles (all of 6, read in 5)
4. Listen to the DS (and don't ignore its wishes)
5. And do your duty as DC (or DP) (and be good)

6. And remember: accountability; GDPR compliance does not happen by accident

Actually: just remember this slide and you are off to a good start!

The GDPR

Questions so far, before we move on to Blockchain?

Blockchain

Many forms exist, but the <u>current</u> general “apparition”:

- BC as a product of a community (majority)
- Distributed / decentralized
- Permissioned or permissionless
- Private or Public
- Hashing / Proof of Work ensures integrity of Blockchain
- Security through encryption
- Transactions are append only
- GDPR through hashing / encryption (or not?)

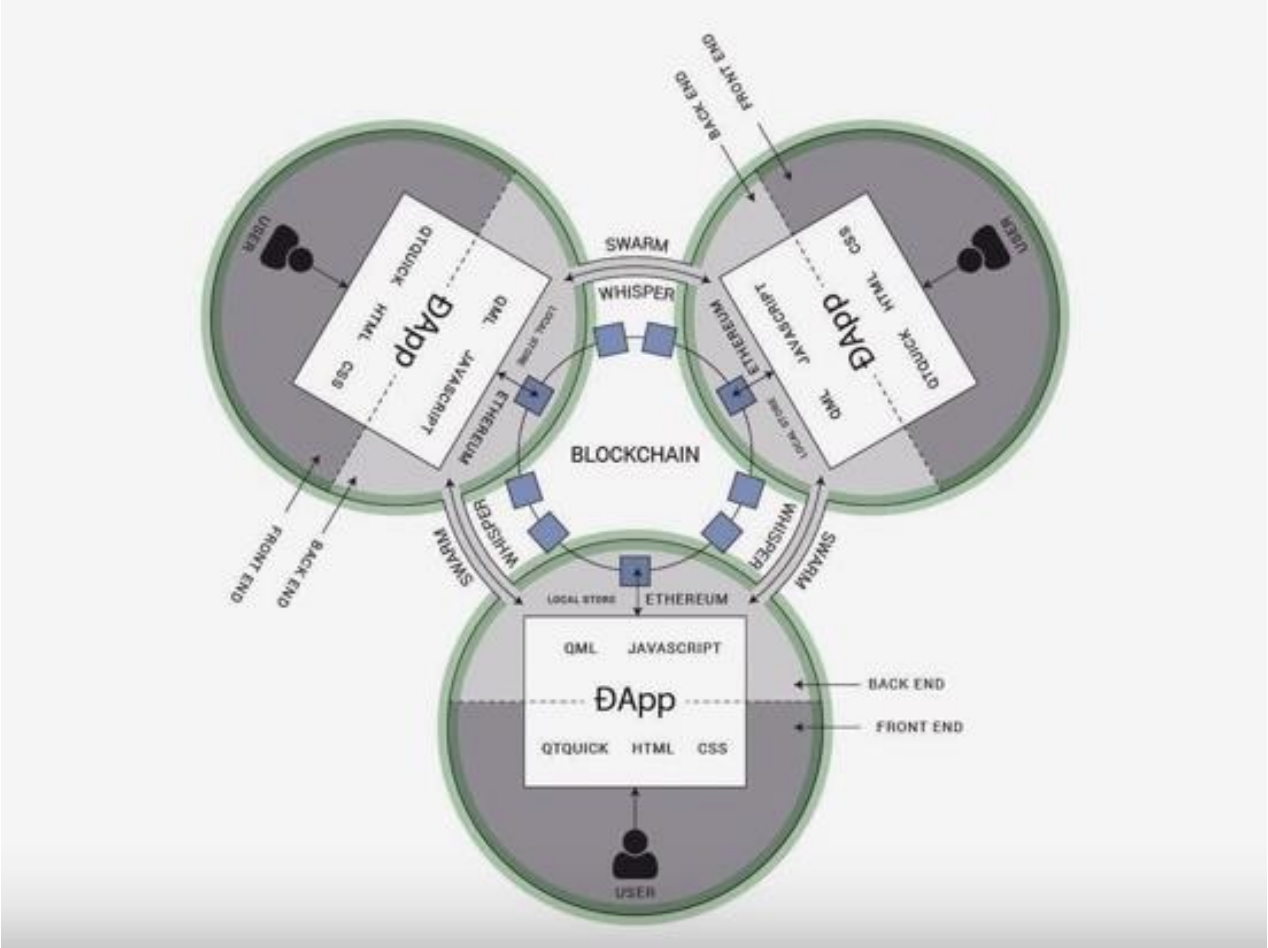
Selected GAPs

GDPR principle (s)	BC principle or application	Blockchain Challenge
GDPR addresses DC and DP	Distributed / Decentralized	Who is DC, difficult to assign roles
Definition of personal data	Hashing / encryption	What is enough / separation of Tr. & PD?
Lawfulness, fairness and transparency, Purpose limitation, Data minimisation, Accuracy, Storage limitation, Integrity and confidentiality	Distributed nodes, community (consensus) determines rules	Q: How to implement rules that are compliant? A: in design and technology, client / DApp DC is responsible!
Erasure Rectification	Immutability	Currently in general not possible … unless (DAO)
Accountability	Community	Nobody or everybody is accountable for BC, DC for transaction?

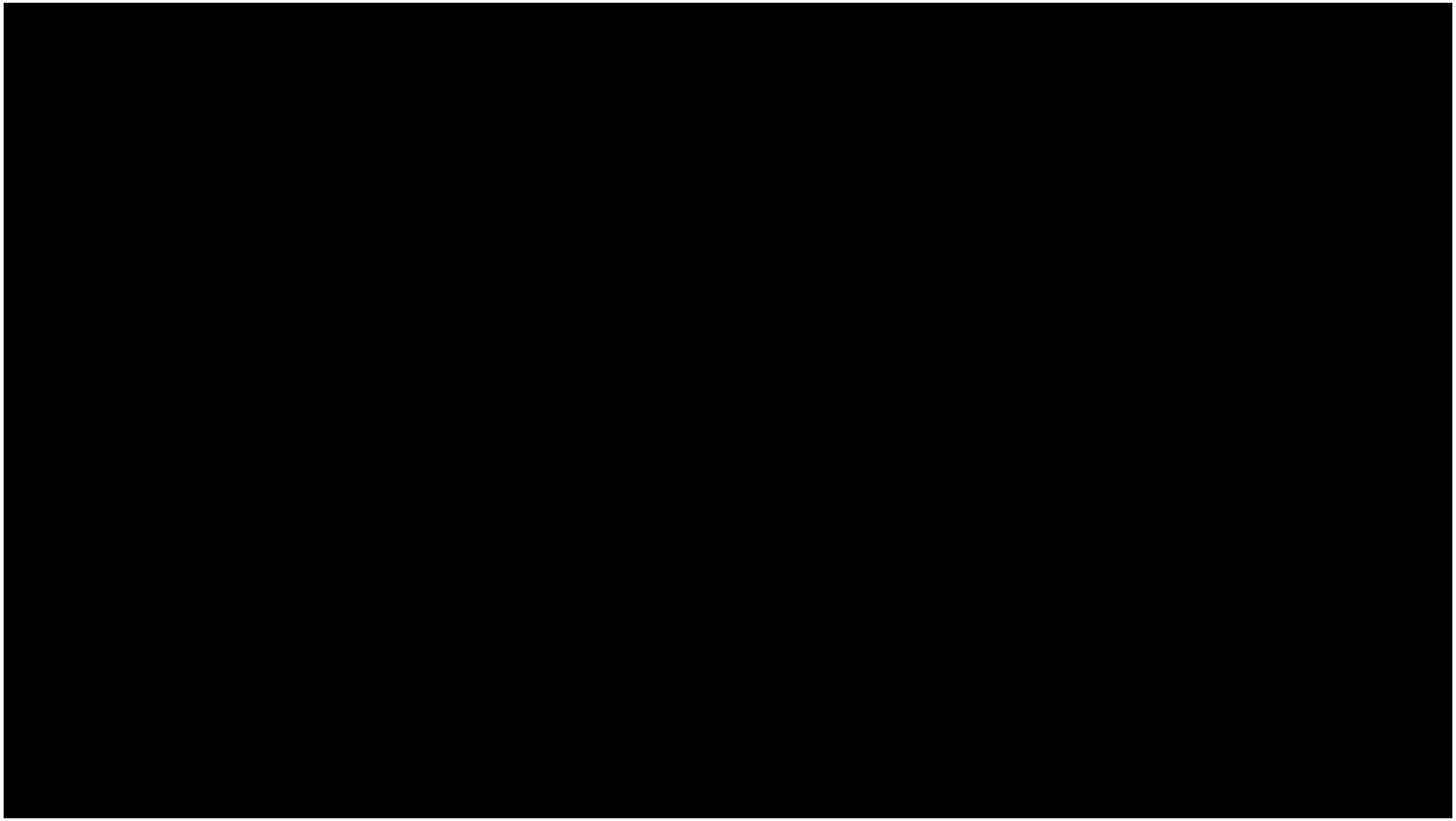
Some observations

a) Assumption, PD is processed
   a) What is PD … multiplayer layers of protection still PD?
   b) Anonymity … then the GDPR is NOT applicable!
b) Many BC apparitions are most likely not GDPR compliant
c) What makes a Node, and is a Node always a DC?
d) Difference between Nodes / DApp's and Services
   a) at least at a transaction level (DC determines purpose and means) which means a DC can be held accountable for compliancy with GDPR?
   b) At a protocol level? one can argue joint controllership (consensus)

Selected GAPs: D’App as solution?



Selected GAPs: Use Case



Some observations

So what if it is decided that current BC apparitions are not compliant?

a) Who should act?

b) Who should the acts be directed against?

   a) Think Brein /Ziggo: should ISP's be directed to block BC traffic? Will that even be possible without DPI?

The End

Your thoughts and Questions?

C/M/S/ Law-Now™

Your free online legal information service.

A subscription service for legal articles
on a variety of topics delivered by email.
www.cms-lawnow.com

C/M/S/ e-guides

Your expert legal publications online.

In-depth international legal research
and insights that can be personalised.
eguides.cmslegal.com

CMS locations:
Aberdeen, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Berlin, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Dubai, Duesseldorf, Edinburgh, Frankfurt, Geneva, Glasgow, Hamburg, Hong Kong, Istanbul, Kyiv, Leipzig, Lisbon, Ljubljana, London, Luxembourg, Lyon, Madrid, Mexico City, Milan, Moscow, Munich, Muscat, Paris, Podgorica, Prague, Rio de Janeiro, Rome, Sarajevo, Seville, Shanghai, Sofia, Strasbourg, Stuttgart, Tehran, Tirana, Utrecht, Vienna, Warsaw, Zagreb and Zurich.

---

www.cmslegal.com